

Reconciling  
Information Exchange  
and Confidentiality  
A Formal Approach

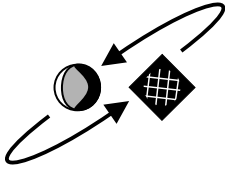
Wouter Teepe



## Rijksuniversiteit Groningen

The research reported in this thesis has been funded by the University of Groningen.

<http://www.rug.nl>



### Department of Artificial Intelligence

The research reported in this thesis has been carried out at the Multi-Agent Systems group (MAS) of the research institute for Artificial Intelligence and Cognitive Engineering (ALICE) of the University of Groningen.

<http://www.ai.rug.nl>



### SIKS Dissertation Series No. 2007-02

The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

<http://www.siks.nl>



The research reported in this thesis has been carried out by Wouter Teepe. <http://www.teepe.com>

Paronyms: Judith Grob & Leendert van Maanen

The author can be reached at [wouter@teepe.com](mailto:wouter@teepe.com)  
Supplemental material and errata will be published at <http://www.teepe.com/phdthesis>

© 2006 Wouter Teepe  
photo back cover: Jeroen van Kooten  
cover design: Frans Boon

NUR: 993, 995

	printed edition	electronic edition
ISBN-10	90-367-2810-X	90-367-2811-8
ISBN-13	978-90-367-2810-2	978-90-367-2811-9

RIJKSUNIVERSITEIT GRONINGEN

# Reconciling Information Exchange and Confidentiality A Formal Approach

Proefschrift

ter verkrijging van het doctoraat in de  
Gedrags- en Maatschappijwetenschappen  
aan de Rijksuniversiteit Groningen  
op gezag van de  
Rector Magnificus, dr. F. Zwarts,  
in het openbaar te verdedigen op  
donderdag 18 januari 2007  
om 14.45 uur

door

Wouter Gerard Teepe

geboren op 23 februari 1977  
te Darmstadt

Promotor: prof.dr. L.R.B. Schomaker  
Copromotor: dr. L.C. Verbrugge

Beoordelingscommissie: prof. dr. W. van der Hoek  
prof. dr. B.P.F. Jacobs  
prof. dr. J.-J. Ch. Meyer  
prof. dr. G.R. Renardel de Lavalette

to Lotte and Lucie



# Contents

<b>I Introduction</b>	<b>1</b>
1 Introduction	3
2 Preliminaries	17
<b>II Tools</b>	<b>27</b>
3 Cryptographic Hash Functions	29
4 Authentication Logics	47
5 ‘Unsoundness’ of BAN logic	55
6 Extending GNY Logic	67
<b>III Approaches</b>	<b>79</b>
7 Information Designators	81
8 Knowledge Authentication	101
<b>IV Protocols</b>	<b>121</b>
9 1-to-many Protocols (T-1)	123
10 Many-to-many Protocols (T-2)	145
<b>V Conclusion</b>	<b>169</b>
11 Conclusion	171
<b>VI Appendices</b>	<b>177</b>
A Remarks to Authentication Logics	179
B Summary of GNY Logic	183
C Remarks to Knowledge Authentication	187
D The Secret Prover	191
E Notation	207
Bibliography	211
Author Index	226
About the Author	234
Samenvatting	235

# Detailed Contents

<b>I</b>	<b>Introduction</b>	<b>1</b>
<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	The Privacy Debate . . . . .	4
1.2	Guarantees of Availability and Confidentiality . . . . .	6
1.3	Thesis Contents . . . . .	8
1.4	Relation to the Author’s Other Publications . . . . .	10
1.5	A Case Study: the Dutch Police . . . . .	10
1.6	Considering Central Storage . . . . .	14
<b>2</b>	<b>Preliminaries</b>	<b>17</b>
2.1	Encryption . . . . .	18
2.2	Authorization and Authentication . . . . .	19
2.3	Complexity . . . . .	20
2.4	Probabilistic Algorithms . . . . .	21
2.5	Oblivious Transfer . . . . .	22
2.6	Adversary Models . . . . .	22
2.7	Secure Multiparty Computation . . . . .	23
2.8	Zero-Knowledge Proofs . . . . .	24
<b>II</b>	<b>Tools</b>	<b>27</b>
<b>3</b>	<b>Cryptographic Hash Functions</b>	<b>29</b>
3.1	Normal Hash Functions . . . . .	30
3.2	Special Properties . . . . .	32
3.3	The Random Oracle Model . . . . .	36
3.4	Design Paradigms . . . . .	37
3.5	Common Applications . . . . .	41
3.6	(Non-) Incrementality . . . . .	44
3.7	Conclusion . . . . .	46
<b>4</b>	<b>Authentication Logics</b>	<b>47</b>
4.1	The Goals of an Authentication Logic . . . . .	48
4.2	The Taxonomy of Any Authentication Logic . . . . .	49
4.3	Using an Authentication Logic . . . . .	52
4.4	The BAN Logic Debate . . . . .	54
4.5	Conclusion . . . . .	54
<b>5</b>	<b>‘Unsoundness’ of BAN logic</b>	<b>55</b>
5.1	Cryptographic Hash Functions and Justified Beliefs . . . . .	55
5.2	On the Computational Justification of Beliefs . . . . .	57
5.3	The Two Parrots Protocol . . . . .	58
5.4	Used Inference Rules . . . . .	61



5.5	Proof of ‘Unsoundness’ of BAN logic . . . . .	61
5.6	The Semantic Approach . . . . .	63
5.7	Conclusion . . . . .	66
<b>6</b>	<b>Extending GNY Logic</b> . . . . .	<b>67</b>
6.1	Why Authentication Logics Are So Tricky . . . . .	67
6.1.1	Unstated Assumptions: Length-Concealment and Non-Incrementality . . . . .	67
6.1.2	Omitted Inference Rules: The Key to Incompleteness . . . . .	69
6.2	Proofs of Knowledge and Ignorance . . . . .	71
6.2.1	New Inference Rules for Proving Possession . . . . .	72
6.2.2	Proving That Principals Do Not Learn Too Much . . . . .	75
6.3	Conclusion . . . . .	77
<b>III</b>	<b>Approaches</b> . . . . .	<b>79</b>
<b>7</b>	<b>Information Designators</b> . . . . .	<b>81</b>
7.1	Information Integration and its Challenges . . . . .	83
7.1.1	Overlapping Ontologies . . . . .	84
7.1.2	Information Propagation . . . . .	85
7.2	A Joint Approach to Privacy, Anonymity and Information Inte- gration . . . . .	87
7.2.1	Information Designators . . . . .	87
7.2.2	Dependency and (Un)linkability . . . . .	88
7.2.3	Operations on Designators . . . . .	89
7.3	An Example: the Datamining Bookshop . . . . .	90
7.3.1	Organizational Setting . . . . .	91
7.3.2	Designators in Action . . . . .	92
7.3.3	Observations About the Use of Subqueries . . . . .	95
7.4	Methods for Restricting Designator Uses . . . . .	96
7.5	Discussion and Related Work . . . . .	98
7.6	Conclusion . . . . .	100
<b>8</b>	<b>Knowledge Authentication</b> . . . . .	<b>101</b>
8.1	Application Areas of Gossip . . . . .	102
8.1.1	Police Investigations . . . . .	102
8.1.2	The Passenger Name Record . . . . .	103
8.2	Comparing Information Without Leaking It and Reference . . . . .	105
8.3	Adversary Models for CIWLI . . . . .	108
8.4	Possible Set Relations . . . . .	109
8.5	Secure Protocols for Computing Set Relations . . . . .	112
8.6	Domain Compression . . . . .	116
8.7	Conclusion . . . . .	119

<b>IV</b>	<b>Protocols</b>	<b>121</b>
<b>9</b>	<b>1-to-many Protocols (T-1)</b>	<b>123</b>
9.1	Prerequisites . . . . .	124
9.2	Protocol Description (Simple, no Encryption) . . . . .	126
9.3	Making the Protocol More Efficient (Elaborate, Encryption) . . . . .	129
9.4	Correctness Proof in GNY Logic . . . . .	133
9.4.1	Knowledge Preconditions . . . . .	134
9.4.2	Claims and GNY Idealization . . . . .	135
9.4.3	The Easy Part of the Proof . . . . .	136
9.4.4	Different Options to Complete the Proof . . . . .	137
9.4.5	Proving principals do not learn too much . . . . .	140
9.4.6	Modeling the beliefs and possessions of an attacker . . . . .	141
9.5	Conclusion . . . . .	142
<b>10</b>	<b>Many-to-many Protocols (T-2)</b>	<b>145</b>
10.1	Using Prefix Trees for Efficiency . . . . .	145
10.2	Specification of the T-2 Protocol . . . . .	148
10.2.1	Subprotocol for Determining Intersection . . . . .	149
10.2.2	Subprotocol for Proving Possession . . . . .	154
10.3	Making the Protocol Efficient by Restrictions . . . . .	157
10.4	Determining Communication Complexity . . . . .	159
10.5	Conclusion . . . . .	166
<b>V</b>	<b>Conclusion</b>	<b>169</b>
<b>11</b>	<b>Conclusion</b>	<b>171</b>
11.1	Information Designators . . . . .	171
11.2	Knowledge Authentication . . . . .	172
11.3	Hash Functions and Authentication Logics . . . . .	174
11.4	Relevance to the Privacy Debate . . . . .	175

<b>VI Appendices</b>	<b>177</b>
<b>A Remarks to Authentication Logics</b>	<b>179</b>
A.1 A Taxonomy of Versions of the BAN Paper	179
A.2 A Short Survey of Criticisms on BAN Logic	180
<b>B Summary of GNY Logic</b>	<b>183</b>
B.1 Formal Language	183
B.2 Inference Rules	184
<b>C Remarks to Knowledge Authentication</b>	<b>187</b>
C.1 The ‘French Approach’	187
C.2 On the Probabilistic Communication Complexity of Set Intersection	188
C.3 Fuzzy Private Matching	189
<b>D The Secret Prover</b>	<b>191</b>
D.1 Starting Up and Connection Control	192
D.1.1 Opening a Connection Listener	193
D.1.2 Making a Connection	193
D.2 Managing Hash Pools	196
D.3 Running the Protocol	198
D.3.1 Initiating a Protocol	199
D.3.2 Responding to a Protocol	200
D.3.3 A Side Note on Hash Pools	200
D.3.4 Challenging	201
D.3.5 Proving	203
D.3.6 Verifying	204
D.3.7 Faking	206
D.4 Closing	206
<b>E Notation</b>	<b>207</b>
E.1 Symbols	207
E.2 Letters	208
<b>Bibliography</b>	<b>211</b>
<b>Author Index</b>	<b>226</b>
<b>SIKS Dissertation Series</b>	<b>230</b>
<b>About the Author</b>	<b>234</b>
<b>Samenvatting</b>	<b>235</b>

## List of Figures

1.1	Dependencies between the chapters that make up the main body of the thesis at hand . . . . .	9
1.2	Matching of police information within the VROS . . . . .	13
2.1	A trivial primality testing algorithm . . . . .	21
2.2	The Miller-Rabin primality testing algorithm . . . . .	21
2.3	A Rubik's cube . . . . .	25
3.1	A 'normal' hash function in action . . . . .	31
3.2	The relation between various properties of cryptographic hash functions . . . . .	35
3.3	A Merkle-Damgård hash function . . . . .	38
3.4	A hash function of the randomize-then-combine paradigm . . . . .	39
3.5	Incremental hash function in action . . . . .	45
4.1	The signing parrot protocol, plain description . . . . .	49
4.2	GNY idealization of the signing parrot protocol . . . . .	51
4.3	GNY annotation of the signing parrot protocol . . . . .	52
4.4	Heavy GNY annotation of the signing parrot protocol . . . . .	53
5.1	The two parrots protocol, graphical illustration. . . . .	58
5.2	The two parrots protocol, plain description . . . . .	60
5.3	BAN idealization of the two parrots protocol . . . . .	60
5.4	GNY idealization of the two parrots protocol . . . . .	60
5.5	Heavy BAN annotation of the two parrots protocol . . . . .	63
7.1	The main aims and interests for organizations participating in information integration . . . . .	86
7.2	An information dependency graph containing the four organizations of the example . . . . .	92
7.3	A global SQL query which would provide the local bookshop with the information it desires . . . . .	94
8.1	The relations possible between two sets $X$ and $Y$ . . . . .	110
8.2	Some interesting set functions for which secure protocols exist . . . . .	110
8.3	Special cases of the sizes of two sets . . . . .	111
9.1	T-1 protocol, no encryption, verifier initiates . . . . .	127
9.2	T-1 protocol, no encryption, prover initiates . . . . .	127
9.3	T-1 protocol, no encryption, mutual proof . . . . .	128
9.4	A rough paraphrase of the T-1 protocols . . . . .	129
9.5	The initialisation and maintenance of the look-up table . . . . .	130
9.6	T-1 protocol, encryption, verifier initiates . . . . .	131
9.7	T-1 protocol, encryption, prover initiates . . . . .	131
9.8	T-1 protocol, encryption, mutual proof . . . . .	132
9.9	GNY idealization of the T-1 protocol, no encryption, verifier initiates . . . . .	136
9.10	The output of the protocol parser for the T-1 protocol . . . . .	137
9.11	GNY proof of the T-1 protocol . . . . .	139

10.1	Sets $KB_A, KB_A$ represented as binary hash value prefix trees . . .	146
10.2	Interleaved subprotocols for establishing the intersection, shown as a colored surface, with $l = 4$ . . . . .	152
10.3	Interleaved subprotocols for establishing the intersection, shown as a colored surface, with $l = 16$ . . . . .	152
10.4	The number of communicated bits in the restricted T-2 protocol with cooperative participants, shown as a density plot . . . . .	163
10.5	The number of communicated bits per compared secret in the restricted T-2 protocol with cooperative participants, shown as a density plot . . . . .	164
D.1	Main application window . . . . .	192
D.2	Opening a connection listener . . . . .	193
D.3	Filling in a name . . . . .	193
D.4	Making a connection . . . . .	194
D.5	Filling in connection details . . . . .	194
D.6	An initiated connection (outgoing) . . . . .	194
D.7	Receiving a connection (incoming) . . . . .	195
D.8	An authentication warning . . . . .	195
D.9	An authentication mismatch . . . . .	195
D.10	Main application window, with connections . . . . .	195
D.11	A new hash pool window . . . . .	196
D.12	Adding files to a hash pool . . . . .	196
D.13	A hash pool with files added . . . . .	196
D.14	Computation of hash values . . . . .	197
D.15	A ready hash pool . . . . .	197
D.16	Adding files to an existing hash pool . . . . .	197
D.17	A new protocol window for the initiator . . . . .	199
D.18	A protocol window, configured by the initiator . . . . .	199
D.19	A protocol window of the initiator for a protocol that has started . . . . .	199
D.20	A new protocol window for the responder . . . . .	200
D.21	The responder has filled in the nonce . . . . .	200
D.22	The responder has committed the nonce . . . . .	200
D.23	The verifier chooses whether he will halt the protocol . . . . .	202
D.24	The verifier has challenged the prover . . . . .	202
D.25	The prover has received a challenge . . . . .	202
D.26	The prover sends some fake hash value $h_2$ . . . . .	203
D.27	The prover sends a genuine hash value $h_2$ . . . . .	203
D.28	The prover has halted the protocol . . . . .	204
D.29	The verifier receives an unexpected value of $h_2$ . . . . .	205
D.30	The verifier receives the $h_2$ he expected . . . . .	205
D.31	The verifier has been informed that the prover has halted the protocol . . . . .	205

## List of Tables

3.1	Some commonly used cryptographic hash functions . . . . .	40
7.1	Two relational tables which can be combined to relate courses to birth dates . . . . .	83
7.2	The schemata of the information that is maintained by the civic authority, the local school and the book publisher . . . . .	93
8.1	All known well-documented secure protocols for computing set relations . . . . .	114
8.2	Protocols which can be used for knowledge authentication . . . . .	116
9.1	Basic messages used in the T-1 protocol. . . . .	125
10.1	Binary encoding of some hash prefix trees . . . . .	147
10.2	Basic messages used in the T-2 protocol . . . . .	148
10.3	A sample run of interleaved subprotocols for establishing the intersection . . . . .	151
10.4	Interleaved subprotocols for establishing the intersection, shown as a growing binary tree . . . . .	153
10.5	State variables in a subprotocol for proving possession . . . . .	155
10.6	A sample run of the subprotocol for proving possession . . . . .	156
10.7	Encoding for sets $R_p$ where $\forall s:  s  = 1$ and $p$ may be omitted . . . . .	158
10.8	A sample protocol run of the restricted T-2 protocol, efficiently encoded . . . . .	159
10.9	The worst case communication complexity for the restricted T-2 protocol, depending on the strategies . . . . .	160
10.10	The ten conditions of the experiment to estimate the average communication complexity of the restricted T-2 protocol with cooperative principals . . . . .	162
10.11	Descriptive statistics of the number of communicated bits in the restricted T-2 protocol with cooperative participants . . . . .	163
10.12	Descriptive statistics of the number of communicated bits per compared secret in the restricted T-2 protocol with cooperative participants . . . . .	164
10.13	Upper bounds on average communication complexities of the T-1 and the T-2 protocol . . . . .	165