Epistemic modelling and protocol dynamics

Wang, Y.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
# Contents

## Acknowledgments

### 1 Introduction

1.1 Background .......................... 2
1.2 Overview of the Dissertation ............... 6
1.3 Origins of the Material .................. 8

### 2 Preliminaries

2.1 Finite Automata and Regular Expressions ........................ 9
2.2 Kripke Models and Bisimulation .................. 10
2.3 Three Logics ................................
  2.3.1 Propositional Dynamic Logic ............... 13
  2.3.2 Epistemic Temporal Logic ................ 15
  2.3.3 Dynamic Epistemic Logic ................. 15

## Logics of Epistemic Protocols

### 3 Meta-knowledge Matters

3.1 Introduction ................................ 21
3.2 Preliminaries ................................ 22
3.3 Announcement Protocol and Verification ............ 24
3.4 Deterministic Protocols for $\text{RCP}_{3,3}$ ............... 29
3.5 Conclusion and Discussion .................. 34

### 4 Logics of Knowledge and Protocol Change

4.1 Introduction ................................ 37
4.2 Basic Logic PDL* ................................ 39
4.3 Public Event Logic PDL* ..................... 43
4.4 Update Logic PDL* .......................... 49
4.5 Conclusion and Future Work .................. 55
IV  Modelling Security Protocols

9  Epistemic Approaches to Security Protocol Verification

9.1  Knowledge in Security Protocols .......................... 139
  9.1.1  Different Aspects of Knowledge ....................... 140
  9.1.2  Tension Between Epistemic and Temporal Structure ..... 141

9.2  Epistemic Approaches: A Brief Survey ..................... 142
  9.2.1  BAN logic ............................................ 142
  9.2.2  Basics of Epistemic Approaches ........................ 143
  9.2.3  Epistemic Temporal Approaches ......................... 145
  9.2.4  Dynamic Epistemic Logic Approaches ................... 148
  9.2.5  Tools ................................................ 149

9.3  Comparisons ................................................ 149
  9.3.1  On Equivalences .................................... 149
  9.3.2  ETL vs. DEL in Modelling ............................ 151

9.4  To Know or Not, Towards a Technical Answer ............... 155
  9.4.1  On Expressivity of ETL .............................. 155
  9.4.2  Model Checking ETL .................................. 157

9.5  Conclusion ................................................. 158

A  Alloy Code for Russian Cards Problem (3.3.1) .................. 159

Bibliography .................................................. 161
Abstract ...................................................... 177
Samenvatting ................................................ 179
Index .......................................................... 181