UvA-DARE (Digital Academic Repository)

Epistemic modelling and protocol dynamics

Wang, Y.

Link to publication

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 xi

1 Introduction 1
   1.1 Background 2
   1.2 Overview of the Dissertation 6
   1.3 Origins of the Material 8

2 Preliminaries 9
   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

I Logics of Epistemic Protocols 19

3 Meta-knowledge Matters 21
   3.1 Introduction 21
   3.2 Preliminaries 22
   3.3 Announcement Protocol and Verification 24
   3.4 Deterministic Protocols for RCP
   3.5 Conclusion and Discussion 34

4 Logics of Knowledge and Protocol Change 37
   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

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Knowledge in Security Protocols</td>
<td>139</td>
</tr>
<tr>
<td>9.1.1</td>
<td>Different Aspects of Knowledge</td>
<td>140</td>
</tr>
<tr>
<td>9.1.2</td>
<td>Tension Between Epistemic and Temporal Structure</td>
<td>141</td>
</tr>
<tr>
<td>9.2</td>
<td>Epistemic Approaches: A Brief Survey</td>
<td>142</td>
</tr>
<tr>
<td>9.2.1</td>
<td>BAN logic</td>
<td>142</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Basics of Epistemic Approaches</td>
<td>144</td>
</tr>
<tr>
<td>9.2.3</td>
<td>Epistemic Temporal Approaches</td>
<td>146</td>
</tr>
<tr>
<td>9.2.4</td>
<td>Dynamic Epistemic Logic Approaches</td>
<td>148</td>
</tr>
<tr>
<td>9.2.5</td>
<td>Tools</td>
<td>149</td>
</tr>
<tr>
<td>9.3</td>
<td>Comparisons</td>
<td>149</td>
</tr>
<tr>
<td>9.3.1</td>
<td>On Equivalences</td>
<td>149</td>
</tr>
<tr>
<td>9.3.2</td>
<td>ETL vs. DEL in Modelling</td>
<td>151</td>
</tr>
<tr>
<td>9.4</td>
<td>To Know or Not, Towards a Technical Answer</td>
<td>155</td>
</tr>
<tr>
<td>9.4.1</td>
<td>On Expressivity of ETL</td>
<td>155</td>
</tr>
<tr>
<td>9.4.2</td>
<td>Model Checking ETL</td>
<td>157</td>
</tr>
<tr>
<td>9.5</td>
<td>Conclusion</td>
<td>158</td>
</tr>
</tbody>
</table>

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

Bibliography | 161

Abstract | 177

Samenvatting | 179

Index | 181