

Contents

1	Introduction	1
1.1	Formal Analysis of Cryptographic Protocols	1
1.2	Protocol Analysis modulo Equational Theories	4
1.3	Reducing the State Search Space	9
1.4	Protocol Composition	12
1.5	Security Properties	14
1.6	Contributions	17
1.7	Plan of the Thesis	19
2	Preliminaries	23
2.1	Rewriting Logic and Term Rewriting	23
2.2	Symbolic Reachability Analysis by Narrowing	29
2.3	Maude	31
3	Maude-NPA	41
3.1	Overview	41
3.2	Maude-NPA's Strand Space Model	43
3.3	Backwards Reachability Analysis	47
3.4	Backwards Operational Semantics	49
3.5	General Requirements for Algebraic Theories	52
3.6	Protocol Specification in Maude-NPA	55
3.6.1	Protocol States	58
3.6.2	Attack States	60
3.7	Maude-NPA Commands	62
4	State Space Reduction in the Maude-NPA	65
4.1	Motivation	66

4.2	Overview of State Space Reduction Techniques	67
4.3	Identifying Unreachable States	69
4.3.1	Grammars	69
4.3.2	Early Detection of Inconsistent States	72
4.4	Redundant States	74
4.4.1	Limiting Dynamic Introduction of New Strands	74
4.4.2	Partial Order Reduction Giving Priority to Input Messages	76
4.4.3	Subsumption Partial Order Reduction	77
4.5	The Super-Lazy Intruder	84
4.5.1	Definition of Super-Lazy Terms	87
4.5.2	The Super-Lazy Intruder and Ghost States	88
4.5.3	Optimizing the Super-Lazy Intruder	94
4.5.4	Transition Subsumption and the Super-Lazy Intruder	94
4.5.5	Implementing Subsumption Partial Order Reduc- tion in the Presence of the Super-Lazy Intruder	97
4.6	Experimental Evaluation	106
4.7	Conclusions	107
5	A Rewriting-based Forwards Semantics for Maude-NPA	113
5.1	Overview	113
5.2	Forward Reachability Analysis	116
5.3	Forwards Operational Semantics	119
5.4	Soundness and Completeness of the Forwards Semantics	126
5.5	Experimental Evaluation	133
5.6	Conclusions	135
6	Sequential Protocol Composition in Maude-NPA	137
6.1	Motivation	138
6.2	Examples of Sequential Protocol Compositions	139
6.2.1	NSL Distance Bounding Protocol	139
6.2.2	NSL Key Distribution Protocol	142
6.3	Abstract Sequential Composition in Maude-NPA	142
6.3.1	Input/Output Parameters and Roles	143
6.3.2	Strand and Protocol Composition	146
6.3.3	Abstract Operational Semantics	150
6.4	Protocol Composition via Protocol Transformation	153

6.4.1	Protocol Transformation	153
6.4.2	Soundness and Completeness of the Protocol Transformation	157
6.5	Protocol Composition via Synchronization Messages . . .	169
6.5.1	Synchronization Data Type Extension	170
6.5.2	Syntax for Protocol Composition via Synchronization Messages	171
6.5.3	Operational Semantics of Composition via Synchronization Messages	174
6.5.4	Soundness and Completeness	178
6.6	Experimental Evaluation	182
6.6.1	The NSL-DB Protocol	182
6.6.2	The NSL-KD Protocol	187
6.6.3	Performance Comparison	189
6.7	Conclusions	191
7	Protocol Indistinguishability in Maude-NPA	193
7.1	Motivation	193
7.2	Formal Definition of Indistinguishability in Maude-NPA .	197
7.2.1	Protocol Pairing	198
7.2.2	Synchronous Product of Protocols	199
7.2.3	Indistinguishability in Maude-NPA	203
7.3	Indistinguishability Verification in Maude-NPA	204
7.4	Experimental Evaluation	207
7.5	Conclusions	211
8	Asymmetric Unification	213
8.1	Motivation	214
8.2	Contextual Symbolic Reachability Analysis	217
8.3	An Asymmetric Unification Algorithm for Exclusive-OR	226
8.3.1	The Inference System	229
8.3.2	The Splitting Rule	230
8.3.3	The Branching Rules	230
8.3.4	Instantiation Rules	232
8.4	Experimental Evaluation	233
8.4.1	Experiments of Contextual Symbolic Analysis of Cryptographic Protocols	233

8.4.2	Experiments with Unification Problems Arising in Protocol Analysis	235
8.5	Conclusions	238
9	Conclusion	239
	Bibliography	243