
Contents

I	Introduction and Objectives	17
1	Introduction	19
1.1	Cryptographic properties	19
1.1.1	Lists-Associativity	20
1.1.2	Exclusive-OR	22
1.1.3	Diffie-Hellman	24
1.1.4	Bilinear Pairing	25
1.1.5	Abelian-Group	27
1.1.6	Constraints	29
1.2	Cryptographic protocol families	30
1.2.1	APIs and Global Mutable Memory	30
1.2.2	Multi-party key agreement protocols	33
1.2.3	Distance bounding protocols	34
1.3	Modeling improvement	35
1.3.1	Constructors	35
1.3.2	Protocol transformation	37
1.4	Objectives and Contributions	38
1.5	Structure of this Thesis	39
1.6	Publications	39
1.7	Research Projects	40
1.8	Research Stays	41

II	Selected Papers	43
2	Formal verification of the YubiKey and YubiHSM APIs in Maude-NPA	45
2.1	Introduction	46
2.2	The YubiKey Device	48
2.3	The YubiHSM Device	52
2.4	Maude-NPA	54
2.4.1	Modeling Mutable Memory by means of Maude-NPA Strand Composition	56
2.4.2	Modeling Event Lists by means of Mutable Memory	58
2.4.3	Modeling Lamport Clocks in Maude-NPA Using Constraints	58
2.5	Formal Specifications in Maude-NPA	59
2.5.1	Formal Specifications of YubiKey in Maude-NPA	59
2.5.2	Formal Specification of YubiHSM in Maude-NPA	60
2.6	Experiments	62
2.6.1	Experiments using Tamarin	63
2.7	Related Work	65
2.8	Conclusions	65
3	An Optimizing Protocol Transformation for Constructor Finite Variant Theories in Maude-NPA	67
3.1	Introduction	68
3.2	Preliminaries	69
3.3	The Maude-NPA	70
3.4	Protocol Transformation	72
3.4.1	Finite Variant Theories	73
3.4.2	Constructor Finite Variant Theories	75
3.5	Case studies	79
3.5.1	The Diffie-Hellman Protocol	79
3.5.2	The STR protocol	81
3.5.3	The Joux Protocol	82
3.5.4	The TAK Group Protocols	83
3.6	Experiments	86
3.7	Conclusions	87

4	Protocol Analysis with Time	91
4.1	Introduction	92
4.2	The Brands-Chaum distance bounding protocol	94
4.3	A Timed Process Algebra	96
4.3.1	New Syntax for Time	96
4.3.2	Timed Intruder Model	100
4.3.3	Timed Process Semantics	101
4.4	Timed Process Algebra into Untimed Process Algebra with Time Variables and Timing Constraints	108
4.5	Timed Process Algebra into Strands in Maude-NPA	111
4.6	Experiments	113
4.7	Conclusions	114
5	Protocol Analysis with Time and Space	117
5.1	Introduction	118
5.1.1	Related work	120
5.2	Two Time and Space Protocols	120
5.3	A Time and Space Process Algebra	125
5.3.1	New Syntax for Location	126
5.3.2	Time and Space Intruder Model	129
5.3.3	Time and Space Process Semantics	131
5.4	Time and Space Process Algebra into Untimed Process Algebra	137
5.5	Timed Process Algebra into Strands in Maude-NPA	142
5.6	Conclusions	148
6	Variant-based Equational Unification under Constructor Symbols	151
6.1	Introduction	152
6.2	Preliminaries	153
6.3	Variant-based Equational Unification in Maude 3.0	155
6.4	Constructor-Root Variant-based Unification	159
6.5	Experimental Evaluation	165
6.6	Conclusion and Future Work	167
III	Conclusions	169
7	Conclusions and Future Work	171