Contents

1. Introduction 1

2. The IITM Model 7
2.1. The General Computational Model 7
2.2. Polynomial Time and Properties of Systems 10
2.3. Notions of Universal Composability 12
2.4. Composition Theorems 13

3. Preliminaries 17
3.1. Notation for the Definition of IITMs 17
3.1.1. Pseudocode 17
3.1.2. Parts of IITMs 17
3.1.3. Running External Code 20
3.2. Standard Security Notions for Cryptographic Primitives 20
3.2.1. Symmetric Encryption 21
3.2.2. Public-Key Encryption 22
3.2.3. Digital Signatures 23
3.2.4. Message Authentication Codes 24
3.2.5. Pseudorandom Functions 25
3.3. Leakage Algorithms 25

4. Modular Protocol Analysis in the IITM Model 29
4.1. Modeling Protocols 30
4.1.1. Addressing of Multiple Sessions 30
4.1.2. Security Proofs Using Composition Theorems 31
4.1.3. Subprotocols and Ideal Functionalities 31
4.1.4. Modeling Corruption 33
4.1.5. Composition with Joint State 34
4.2. Ideal Functionalities for Cryptographic Primitives 37
4.2.1. Public-Key Encryption 39
4.2.2. Digital Signatures 44
4.2.3. Symmetric Encryption 48
4.2.4. Message Authentication Codes 53
4.2.5. Key Derivation 56
4.2.6. Joint State Realizations 59
4.2.7. Nonces 65

4.3. Ideal Functionalities for Key Exchange and Secure Channel Protocols 67
4.3.1. Key Exchange 67
4.3.2. Key Usability 69
4.3.3. Secure Channel 71
4.4. Security Analysis of an Example Protocol 73
4.4.1. Our Simple Key Exchange Protocol (OSKE) 74
4.4.2. Modeling OSKE in the IITM Model 74
4.4.3. Security of OSKE 75
4.4.4. Building Secure Channels from Key Exchange Protocols . . . 80

5. An Ideal Functionality for Cryptographic Primitives 83
5.1. Preliminaries 84
5.1.1. Key Types and Domains 84
5.1.2. Plaintext Formatting and Parsing 85
5.1.3. Salt Parsing 87
5.2. The Ideal Crypto Functionality 87
5.2.1. Parameters 87
5.2.2. Brief Description 88
5.2.3. Detailed Description 90
5.2.4. Detailed Description of the Provided Operations 93
5.2.5. Remarks 99
5.3. Realization of the Ideal Crypto Functionality 101
5.3.1. The Realization 101
5.3.2. Proof of Realization 105
5.4. Joint State Realization of the Ideal Crypto Functionality 110
5.5. Related Work 112

6. Computational Soundness for KE Protocols with Symmetric Encryption 115
6.1. The Symbolic Model 116
6.1.1. Syntax 117
6.1.2. Operational Semantics 119
6.1.3. Deduction, Static Equivalence, and Labeled Bisimilarity . . . 120
6.2. Symbolic Protocols 122
6.3. Computational Interpretation of Symbolic Protocols 124
6.4. The Computational Soundness Result 131
6.5. Proof of the Computational Soundness Result 135
6.5.1. Mapping Lemmas 136
6.5.2. Proof of Theorem 6.1 145
6.6. Related Work 148

7. Protocol Analysis Without Pre-Established Session Identifiers 151
7.1. On the Role of SIDs in Universal Composition Theorems 152
7.2. Multi-Session Local-SID Ideal Functionalities 154
7.3. Multi-Session Real Protocols 158

7.4. Analyzing Key Exchange Protocols based on our Crypto Functionality 160
7.4.1. Key Exchange Protocols 161
7.4.2. A Criterion for Secure Key Exchange Protocols 163
7.4.3. Application: Security Analysis of the 4WHS protocol of WPA2 170
7.5. Universal Composition Without Pre-Established SIDs 178
7.5.1. Class of Real Protocols 178
7.5.2. Single-Session Realizability 180
7.5.3. The Universal Composition Theorem 182
7.6. Joint State Composition Without Pre-Established SIDs 183
7.6.1. Preliminaries 185
7.6.2. Implicit Disjointness 195
7.6.3. The Composition Theorem with Joint State 200
7.7. Applications of our Composition Theorems 202
7.7.1. Applications to Key Exchange and Secure Channel Protocols 202
7.7.2. Case Studies on Real-World Security Protocols 203
7.8. Related Work 225

8. Conclusion 227

Bibliography 229

A. Realizations of Long-Term Key Functionalities 241
A.1. Proof of Theorem 4.3 241
A.2. Proof of Theorem 4.4 246
A.3. Proof of Theorem 4.5 248

B. Details and a Proof for our Crypto Functionality 253
B.1. Formal Specification of the Ideal Crypto Functionality 253
B.2. Proof of Theorem 5.1 261

C. Details and Proofs for our Computational Soundness Result 273
C.1. Computational Interpretation of Symbolic Protocols 273
C.2. Applications 277
C.2.1. Our Simple Key Exchange Protocol (OSKE) 277
C.2.2. The ANSSK' Protocol 279
C.3. Proof of Lemma 6.3 282
C.3.1. Proof of (6.1) and (6.2) 282
C.3.2. Proof of (6.3) 285
C.4. Proof of Corollary 6.2 286

D. Details and Proofs for Protocol Analysis Without Pre-Established SIDs 289
D.1. Proof of Theorem 7.4 289
D.2. Proof of Theorem 7.5 300
D.2.1. Step 1: $\mathcal{E} \mid \mathcal{P} \mid \widetilde{\mathcal{F}}_{\text{crypto}} \equiv \mathcal{E} \mid \mathcal{Q}_\tau$ 301

D.2.2. Step 2: $\mathcal{E} \mid \mathcal{Q}_\tau \equiv \mathcal{E} \mid \mathcal{S} \mid \mathcal{F}$ 314
D.3. Applications 319
D.3.1. The Needham-Schroeder Public-Key Protocol 320
D.3.2. Building Secure Channels from Key Exchange Protocols . . . 321
D.3.3. Collision Resistant Hash functions 327