

Information Security and Cryptography

Series Editors

David Basin
Kenny Paterson

Advisory Board

Michael Backes
Gilles Barthe
Ronald Cramer
Ivan Damgård
Andrew D. Gordon
Joshua D. Guttman
Christopher Kruegel
Ueli Maurer
Tatsuaki Okamoto
Adrian Perrig
Bart Preneel

Colin Boyd • Anish Mathuria • Douglas Stebila

Protocols for Authentication and Key Establishment

Second Edition

 Springer

Colin Boyd
Department of Information Security
and Communication Technology
Norwegian University of Science
and Technology
Trondheim, Norway

Anish Mathuria
Dhirubhai Ambani Institute
of Information and Communication
Technology (DA-IICT)
Gandhinagar, Gujarat, India

Douglas Stebila
Department of Combinatorics
and Optimization
University of Waterloo
Waterloo, ON, Canada

Originally published under: Boyd C. and Mathuria A.

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-662-58145-2 ISBN 978-3-662-58146-9 (eBook)
<https://doi.org/10.1007/978-3-662-58146-9>

© Springer-Verlag GmbH Germany, part of Springer Nature 2003, 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.

The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

To the memory of my father
Thou thy worldly task hast done
– *CB*

To the memory of my grandmother
– *AM*

To my parents and teachers
– *DS*

Preface

The first edition of this book was published in 2003. Inevitably, certain parts of the book became outdated quickly. At the same time new developments have continued apace, including new concrete protocols, new understanding of protocol security properties, and new cryptographic primitives and techniques which can be used in protocol design. Work on a new edition began as early as 2010, but even as it was being written its scope expanded. We are aware that some important protocols have been omitted, and that there are emerging areas which will see considerable activity in the near future (post-quantum secure protocols being one obvious example). However, we still hope that we have been able to capture most of the main developments that have occurred since the first edition.

This second edition has broadly the same purpose and scope as the first edition. We hope to provide a helpful reference for the expert while still being accessible to those newer to the topic, including those trying to obtain a broad overview of the field. In comparison with the first edition, there are three new chapters and all the other chapters (one renamed) have been extensively revised. The new book is around 50% larger with around 225 concrete protocols described and a bibliography with almost twice as many references. Some older material, which we deemed less relevant today, has been removed.

Chapter 1 replaces the first two chapters from the first edition. The chapter is intended to provide the necessary background on cryptography, attack scenarios and protocol goals with an expanded coverage. The initial tutorial introduction has been moved to an appendix, while some parts of Chapter 2 from the first edition were removed as they seemed no longer relevant. An updated, but somewhat shortened, introduction to protocol verification is also included.

Chapter 2 is the first completely new chapter, describing computational models for key exchange and authentication. The purpose of this chapter is not to provide a tutorial on how to read, let alone write, computational proofs, but rather to try to help readers understand what a computational proof provides and how to compare the many different computational models in use. In later chapters we

have freely made reference to the major computational models when discussing specific protocols and their security.

Chapter 3 is an updated chapter covering protocols using shared key cryptography. This includes major updates on the status of the protocols in the ISO 9798-2 and 11770-2 standards.

Chapter 4 is an updated chapter on protocols using public key cryptography. Again, this includes new developments of the ISO standard protocols, this time for the 9798-3 and 11770-3 protocols. Coverage of TLS is moved to the new Chap. 6 which is devoted to TLS.

Chapter 5 on key agreement is, as in the first edition, the longest chapter. There is an amazing diversity of ideas in design of key agreement protocols, even in the simplest case covered in this chapter, which is limited to two-party protocols in the public key setting. Even though several older protocols from the first edition have been omitted, the revised chapter is now more than ten pages longer, illustrating that there are still many new developments occurring.

Chapter 6 is a completely new chapter on the TLS protocol. As the most prominent key establishment protocol in use today, we believe it is more than justifiable to devote a chapter to TLS. The development of the protocol in the past 10 years, culminating in the new TLS 1.3 protocol, provides many lessons for those researching and implementing key establishment protocols.

Chapter 7 is the third new chapter and is dedicated to ID-based protocols. While it gathers in some early ID-based protocols already included in the first edition, the coverage of pairing-based protocols forms the bulk of the chapter and is completely new.

Chapter 8 is an updated chapter on password-based protocols. This is another topic where there has been a great deal of research activity since the first edition leading to a significant expansion in the chapter.

Chapter 9 is an updated (and renamed) chapter on group key establishment. Although group protocols have a long history there has been much recent work to modernise the topic with stronger security properties and formal proofs.

Appendix A covers standards for key establishment and authentication protocols from various standards bodies, updated and expanded from the first edition.

Appendix B consists of a tutorial introduction to protocols for authentication and key establishment. This is unchanged from the corresponding section in the first edition, apart from some small notational revisions.

Acknowledgements

Many people have given their help and advice generously to help us to improve the quality of the book. Different people have reviewed and provided comment on various portions of the book. We thank them all for their generous spirit and are sincerely sorry if we have misinterpreted or forgotten any of their helpful advice. This list includes all those who we can remember; we hope not to have missed anyone.

Craig Costello
Tibor Jager
Kenneth Radke

Sigurd Eskeland
Chris Mitchell
SeongHan Shin

Håkon Jacobsen
Ruxandra Olimid
Berkant Ustaoglu

In addition, Kazuki Yoneyama provided helpful answers to specific questions. We are solely responsible for all errors of fact, presentation style, or just plain typing errors that this book may have.

The team at Springer have been encouraging and helpful throughout. We would particularly like to thank Ronan Nugent for his unfailing confidence and quick action on all matters, even as we delayed time and again. Series editor Kenny Paterson provided enthusiastic and encouraging support.

CB would like to record his personal thanks to his family for bearing with denial of service during the seemingly interminable saga of the second edition. When the work started he was with Queensland University of Technology, particularly the School of Electrical Engineering and Computer Science. More recently he has been at the Norwegian University of Science and Technology in the department now called Information Security and Communication Technology. Both institutions have provided encouragement and resources to support this work.

AM would like to express his gratitude to his wife, Hemal, and daughter, Radhika, for their unfailing love, support, and patience. His work was carried out at the University of Massachusetts at Dartmouth and more recently at the Dhirubhai Ambani Institute of Information and Communication Technology. He would like to thank his colleagues at both of these institutions for their support and encouragement.

DS would like to thank CB and AM for inviting him to join them in updating the fine work they did in the first edition. This work has been carried out over his time at the Queensland University of Technology, McMaster University, and now the University of Waterloo, and colleagues at all of these were supportive of his work on this project.

This book was typeset in $\text{\LaTeX}$ on various platforms. The style for the protocols and attacks is adapted from Anselm Lingnau's float package.

Trondheim, Gandhinagar, Waterloo
January 2019

*Colin Boyd
Anish Mathuria
Douglas Stebila*

Contents

List of Protocols XXI

List of Attacks XXVII

1 Introduction to Authentication and Key Establishment 1

1.1 Introduction 1

1.2 Protocol Architectures 2

1.2.1 Cryptographic Keys 2

1.2.2 Method of Session Key Generation 3

1.2.3 Number of Parties 4

1.2.4 Example 4

1.3 Cryptographic Tools 5

1.3.1 Confidentiality 6

1.3.2 Data Origin Authentication and Data Integrity 8

1.3.3 Authenticated Encryption 9

1.3.4 Non-repudiation 9

1.3.5 Examples of Cryptographic Algorithms 10

1.3.6 Secret Sharing 11

1.3.7 Freshness Mechanisms 12

1.4 Adversary Capabilities 14

1.4.1 Eavesdropping 15

1.4.2 Modification 15

1.4.3 Replay 16

1.4.4 Preplay 16

1.4.5 Reflection 16

1.4.6 Denial of Service 17

1.4.7 Typing Attacks 18

1.4.8 Cryptanalysis 20

1.4.9 Certificate Manipulation 20

1.4.10 Protocol Interaction 22

1.5 Goals for Authentication and Key Establishment 22

1.5.1 Models of Security 24

1.5.2	Key Establishment or Authentication?	24
1.5.3	Entity Authentication	26
1.5.4	Key Establishment	28
1.5.5	Key Confirmation	29
1.5.6	Example: STS Protocol	31
1.5.7	Forward Secrecy	33
1.5.8	Weak Forward Secrecy	35
1.5.9	Key Compromise Impersonation	36
1.5.10	Deniability	37
1.5.11	Anonymity	39
1.5.12	Protocol Efficiency	41
1.6	Tools for Verification of Protocols	43
1.6.1	FDR	44
1.6.2	NRL Analyzer and Maude-NPA	47
1.6.3	ProVerif	48
1.6.4	Scyther and Tamarin	48
1.6.5	Tools for Computational Models	50
1.6.6	Comparison of Tools	51
1.7	Conclusion	52
2	Computational Security Models	53
2.1	Introduction	53
2.1.1	The Significance of a Computational Proof of Security	54
2.1.2	Elements of Computational Models	55
2.2	Bellare–Rogaway Model	58
2.2.1	BR93: The First Computational Model	58
2.2.2	BR95: Server-Based Protocols	65
2.2.3	The Public Key Setting: The BWM and BWJM Models	66
2.2.4	BPR00: Forward Secrecy and Passwords	67
2.2.5	Summarising the BR Model Variants	69
2.3	Canetti–Krawczyk Model	69
2.3.1	BCK98 Model	69
2.3.2	CK01 Model	70
2.3.3	HMQV Model	75
2.4	eCK Model	76
2.4.1	MU08 Model	78
2.4.2	eCK-PFS Model	78
2.4.3	seCK Model	79
2.5	Comparing Computational Models for Key Exchange	79
2.5.1	Comparing the BR and CK Models	80
2.5.2	Comparing eCK and Other Models	81
2.5.3	Sessions and Session Identifiers	82
2.5.4	Incorporating Public Key Infrastructure	83
2.6	Shoup’s Simulation Model	84
2.7	Models for Enhanced Scenarios	85

2.7.1	Models for Group Key Exchange	86
2.7.2	Models for Multi-factor Key Exchange	87
2.8	Secure Channels	88
2.8.1	CK01 Secure Channels	89
2.8.2	CK02 Secure Channels	91
2.8.3	Authenticated and Confidential Channel Establishment (ACCE) Protocols	91
2.9	Conclusion	93
3	Protocols Using Shared Key Cryptography	95
3.1	Introduction	95
3.2	Entity Authentication Protocols	96
3.2.1	Bird–Gopal–Herzberg–Janson–Kutten–Molva–Yung Protocols	97
3.2.2	Bellare–Rogaway MAP1 Protocol	98
3.2.3	ISO/IEC 9798-2 Protocols	99
3.2.4	ISO/IEC 9798-4 Protocols	101
3.2.5	Woo–Lam Authentication Protocol	102
3.2.6	Comparison of Entity Authentication Protocols	103
3.3	Server-Less Key Establishment	104
3.3.1	Andrew Secure RPC Protocol	104
3.3.2	Janson–Tsudik 2PKDP Protocol	106
3.3.3	Boyd Two-Pass Protocol	107
3.3.4	ISO/IEC 11770-2 Server-Less Protocols	108
3.3.5	Comparison of Server-Less Protocols	110
3.4	Server-Based Key Establishment	110
3.4.1	Needham–Schroeder Shared Key Protocol	111
3.4.2	Otway–Rees Protocol	113
3.4.3	Kerberos Protocol	115
3.4.4	ISO/IEC 11770-2 Server-Based Protocols	117
3.4.5	Wide-Mouthed-Frog Protocol	122
3.4.6	Yahalom Protocol	122
3.4.7	Janson–Tsudik 3PKDP Protocol	125
3.4.8	Bellare–Rogaway 3PKD Protocol	126
3.4.9	Woo–Lam Key Transport Protocol	126
3.4.10	Gong Key Agreement Protocols	127
3.4.11	Boyd Key Agreement Protocol	129
3.4.12	Gong Hybrid Protocol	129
3.4.13	Comparison of Server-Based Protocols	130
3.5	Key Establishment Using Multiple Servers	132
3.5.1	Gong’s Multiple Server Protocol	132
3.5.2	Chen–Gollmann–Mitchell Protocol	133
3.6	Conclusion	134

4	Authentication and Key Transport Using Public Key Cryptography . .	135
4.1	Introduction	135
4.1.1	Notation	136
4.1.2	Design Principles for Public Key Protocols	137
4.2	Entity Authentication Protocols	137
4.2.1	Protocols in ISO/IEC 9798-3	138
4.2.2	Protocols in ISO/IEC 9798-5	142
4.2.3	SPLICE/AS	142
4.2.4	Comparison of Entity Authentication Protocols	143
4.3	Key Transport Protocols	144
4.3.1	Protocols in ISO/IEC 11770-3	144
4.3.2	Blake-Wilson and Menezes Key Transport Protocol	149
4.3.3	Needham-Schroeder Public Key Protocol	150
4.3.4	Needham-Schroeder Protocol Using Key Server	152
4.3.5	Protocols in the X.509 Standard	153
4.3.6	Public Key Kerberos	155
4.3.7	Beller-Chang-Yacobi Protocols	156
4.3.8	TMN Protocol	160
4.3.9	AKA Protocol	161
4.3.10	Comparison of Key Transport Protocols	163
4.4	Conclusion	164
5	Key Agreement Protocols	165
5.1	Introduction	165
5.1.1	Key Derivation Functions	166
5.1.2	Key Control	167
5.1.3	Unknown Key-Share Attacks	167
5.1.4	Classes of Key Agreement	168
5.1.5	Protocol Compilers for Key Agreement	169
5.2	Diffie-Hellman Key Agreement	169
5.2.1	Small Subgroup Attacks	173
5.2.2	ElGamal Encryption and One-Pass Key Establishment	173
5.2.3	Lim-Lee Protocol Using Static Diffie-Hellman	175
5.3	MTI Protocols	176
5.3.1	Small Subgroup Attack	178
5.3.2	Unknown Key-Share Attacks	179
5.3.3	Lim-Lee Attack	181
5.3.4	Impersonation Attack of Just and Vaudenay	182
5.3.5	Triangle Attacks	182
5.3.6	Yacobi's Protocol	183
5.3.7	Forward Secrecy and Key Compromise Impersonation	184
5.4	Diffie-Hellman-Based Protocols with Basic Message Format	185
5.4.1	KEA Protocol	186
5.4.2	Ateniese-Steiner-Tsudik Protocol	187
5.4.3	Just-Vaudenay-Song-Kim Protocol	188

5.4.4	Unified Model Protocol	190
5.4.5	MQV Protocol	191
5.4.6	HMQV Protocol	193
5.4.7	NAXOS Protocol	196
5.4.8	CMQV Protocol	198
5.4.9	NETS and SMEN	199
5.4.10	Protocol of Kim, Fujioka, and Ustaoglu	201
5.4.11	OAKE Protocol	202
5.4.12	Moriyama–Okamoto Protocols	203
5.4.13	Adding Key Confirmation	204
5.4.14	Comparison of Basic Diffie–Hellman Protocols	205
5.5	Diffie–Hellman Protocols with Explicit Authentication	207
5.5.1	Generic Constructions for Authenticated Diffie–Hellman	208
5.5.2	STS Protocol	209
5.5.3	Oakley Protocol	212
5.5.4	SKEME Protocol	215
5.5.5	Internet Key Exchange	216
5.5.6	SIGMA and Internet Key Exchange v2 (IKEv2)	221
5.5.7	Just Fast Keying	223
5.5.8	Arazi’s Protocol	225
5.5.9	Lim–Lee Protocols	226
5.5.10	Hirose–Yoshida Protocol	228
5.5.11	Jeong–Katz–Lee TS3 Protocol	229
5.5.12	YAK Protocol	229
5.5.13	DIKE Protocol	231
5.5.14	Comparison of Authenticated Diffie–Hellman Protocols	232
5.6	Protocols in ISO/IEC 11770-3	233
5.7	Diffie–Hellman Key Agreement in Other Groups	234
5.8	Protocols Based on Encryption or Encapsulation	235
5.8.1	SKEME without Forward Secrecy	236
5.8.2	Boyd–Cliff–González–Nieto–Paterson Protocol	237
5.8.3	Fujioka–Suzuki–Xagawa–Yoneyama Protocol	238
5.8.4	Alawatugoda Protocol	239
5.9	Conclusion	240
6	Transport Layer Security Protocol	241
6.1	Internet Security Protocols	241
6.2	Background on TLS	242
6.3	Protocol Structure	243
6.3.1	Handshake Protocol	244
6.3.2	Record Layer Protocol	249
6.4	Additional Functionality	250
6.4.1	Compression	251
6.4.2	Session Resumption	251
6.4.3	Renegotiation	252

6.5	Variants	252
6.6	Implementations	254
6.7	Security Analyses	255
6.7.1	Provable Security	255
6.7.2	Formal Methods	257
6.8	Attacks: Overview	258
6.9	Attacks: Core Cryptography	259
6.9.1	Bleichenbacher's Attack on PKCS#1v1.5 RSA Key Transport	259
6.9.2	Bleichenbacher's Attack on PKCS#1v1.5 RSA Signature Verification	262
6.9.3	Weaknesses in DES, Triple-DES, MD5, and SHA-1	263
6.9.4	RC4 Biases	264
6.9.5	Weak RSA and Diffie–Hellman: FREAK and Logjam Attacks	266
6.10	Attacks: Crypto Usage in Ciphersuites	268
6.10.1	BEAST Adaptive Chosen Plaintext Attack and POODLE ...	268
6.10.2	Cross-Protocol Attack on Diffie–Hellman Parameters	271
6.10.3	Lucky 13 Attack on MAC-Then-Encode-Then-Encrypt ...	272
6.11	Attacks: Protocol Functionality	273
6.11.1	Downgrade Attacks	273
6.11.2	Renegotiation Attack	274
6.11.3	Compression-Related Attacks: CRIME, BREACH	277
6.11.4	Termination Attack	278
6.11.5	Triple Handshake Attack	279
6.12	Attacks: Implementations	280
6.12.1	Side Channel Attacks	280
6.12.2	TLS-Specific Implementation Flaws	281
6.12.3	Certificate Validation	281
6.12.4	Bad Random Number Generators	282
6.13	Attacks: Other	283
6.13.1	Application-Level Protocols	283
6.13.2	Certificate Authority Breaches and Related Flaws	284
6.14	TLS Version 1.3	285
7	Identity-Based Key Agreement	289
7.1	Introduction	289
7.1.1	Security Model for Identity-Based Cryptosystems	290
7.1.2	Elliptic Curve Pairings	291
7.1.3	Sakai–Ohgishi–Kasahara Protocol	293
7.2	Identity-Based Protocols without Pairings	294
7.2.1	Okamoto's Scheme	295
7.2.2	Günther's Scheme	297
7.2.3	Fiore–Gennaro Scheme	299
7.2.4	Comparison	301
7.3	Pairing-Based Key Agreement with Basic Message Format	302
7.3.1	Smart's Protocol	303

7.3.2	Variants of Smart's Protocol	304
7.3.3	Ryu–Yoon–Yoo Protocol	305
7.3.4	Shim's Protocol	306
7.3.5	Scott's Protocol	308
7.3.6	Chen–Kudla Protocol	309
7.3.7	Wang's Protocol (IDAK)	310
7.3.8	McCullagh–Barreto Protocol	311
7.3.9	Comparison	313
7.4	Pairing-Based Key Agreement with Explicit Authentication	315
7.4.1	Boyd–Mao–Paterson Protocol	315
7.4.2	Asymmetric Protocol of Choi <i>et al.</i>	316
7.4.3	Identity-Based Key Agreement without Random Oracles	317
7.4.4	Comparison	318
7.5	Identity-Based Protocols with Additional Properties	319
7.5.1	Using Multiple KGCs	319
7.5.2	Girault's Three Levels	321
7.5.3	Certificateless Key Agreement	324
7.5.4	Protocols with Generalised Policies	325
7.5.5	One-Pass Identity-Based Protocols	325
7.6	Conclusion	327
8	Password-Based Protocols	329
8.1	Introduction	329
8.2	Encrypted Key Exchange Using Diffie–Hellman	332
8.2.1	Bellovin and Merritt's Original EKE	332
8.2.2	Augmented EKE	335
8.3	Two-Party PAKE Protocols	337
8.3.1	PAK	337
8.3.2	SPEKE	340
8.3.3	Dragonfly Protocol	342
8.3.4	SPAKE	343
8.3.5	J-PAKE	345
8.3.6	Katz–Ostrovsky–Yung Protocol	347
8.3.7	Protocol of Jiang and Gong	347
8.3.8	Protocols Using Smooth Projective Hashing	348
8.3.9	Protocols Using a Server Public Key	351
8.3.10	Comparing Two-Party PAKE Protocols	354
8.4	Two-Party Augmented PAKE Protocols	356
8.4.1	PAK-X, PAK-Y and PAK-Z	357
8.4.2	B-SPEKE	357
8.4.3	SRP	359
8.4.4	AMP	362
8.4.5	AugPAKE Protocol	363
8.4.6	Using Multiple Servers	364
8.4.7	Comparing Two-Party Augmented PAKE Protocols	365

8.5	RSA-Based Protocols	365
8.5.1	RSA-Based EKE	366
8.5.2	OKE and SNAP1	367
8.6	Three-Party PAKE Protocols	369
8.6.1	GLNS Secret Public Key Protocols	369
8.6.2	Steiner, Tsudik and Waidner Three-Party EKE	373
8.6.3	GLNS Protocols with Server Public Keys	375
8.6.4	Three-Party Protocol of Yen and Liu	376
8.6.5	Generic Protocol of Abdalla, Fouque and Pointcheval	377
8.6.6	Stronger Security Models for Three-Party PAKE	378
8.6.7	Three-Party Protocol of Yoneyama	379
8.6.8	Cross-Realm PAKE Protocols	380
8.6.9	Comparing Three-Party PAKE Protocols	383
8.7	Group PAKE Protocols	383
8.7.1	Concrete Protocol Constructions	384
8.7.2	Generic Constructions	386
8.8	Conclusion	387
9	Group Key Establishment	389
9.1	Introduction	389
9.1.1	Efficiency in Group Key Establishment	390
9.1.2	Generalised Security Goals	390
9.1.3	Static and Dynamic Groups	392
9.1.4	Insider Attacks	393
9.1.5	Notation	394
9.2	Generalising Diffie–Hellman Key Agreement	394
9.2.1	Ingemarsson–Tang–Wong Key Agreement	395
9.2.2	Steiner–Tsudik–Waidner Key Agreement	396
9.2.3	Steer–Strawczynski–Diffie–Wiener Key Agreement	399
9.2.4	Kim–Perrig–Tsudik Tree Diffie–Hellman	400
9.2.5	Becker and Wille’s Octopus Protocol	402
9.2.6	Burmester–Desmedt Key Agreement	404
9.2.7	One-Round Tripartite and Multi-Party Diffie–Hellman	407
9.2.8	Security of Generalised Diffie–Hellman	407
9.2.9	Efficiency of Generalised Diffie–Hellman	408
9.3	Group Key Agreement Protocols	410
9.3.1	Authenticating Generalised Diffie–Hellman	410
9.3.2	Klein–Otten–Beth Protocol	411
9.3.3	Authenticated GDH Protocols	412
9.3.4	Authenticated Tree Diffie–Hellman	416
9.3.5	Katz–Yung Compiler	416
9.3.6	Protocol of Bohli, Gonzalez Vasco and Steinwandt	419
9.3.7	Authenticated Tripartite Diffie–Hellman	421
9.3.8	Comparing Authenticated Group Diffie–Hellman	422
9.4	Identity-Based Group Key Establishment Protocols	423

9.4.1	Koyama and Ohta Protocols	424
9.4.2	Protocols of Saeednia and Safavi-Naini	427
9.4.3	ID-Based Group Key Agreement and Pairings	428
9.5	Group Key Agreement without Diffie–Hellman	429
9.5.1	Pieprzyk and Li’s Key Agreement Protocol	429
9.5.2	Tzeng–Tzeng Protocols	430
9.5.3	Boyd–González Nieto Group Key Agreement	432
9.5.4	Generic One-Round Group Key Agreement from Multi-KEM	433
9.5.5	Asymmetric Group Key Agreement	434
9.6	Group Key Transport Protocols	434
9.6.1	Burmester–Desmedt Star and Tree Protocols	434
9.6.2	Mayer and Yung’s Protocols	437
9.6.3	Key Hierarchies	439
9.7	Conclusion	440
A	Standards for Authentication and Key Establishment	441
A.1	ISO Standards	441
A.1.1	ISO/IEC 9798	441
A.1.2	ISO/IEC 11770	442
A.1.3	ISO 9594-8/ITU X.509	443
A.2	IETF Standards	443
A.3	IEEE P1363 Standards	444
A.4	NIST Standards	444
A.5	Other Standards and Protocols	446
A.5.1	ANSI	446
A.5.2	Widely Deployed Protocols	447
B	Tutorial: Building a Key Establishment Protocol	449
B.1	Confidentiality	451
B.2	Authentication	453
B.3	Replay	455
B.4	Design Principles for Cryptographic Protocols	459
C	Summary of Notation	461
	References	463
	General Index	513
	Protocol Index	519

List of Protocols

1.1	A protocol in an unusual class	4
1.2	Use of a nonce (random challenge)	13
1.3	A protocol vulnerable to reflection attack	17
1.4	Otway–Rees protocol	19
1.5	A protocol vulnerable to certificate manipulation (MTI protocol)	21
1.6	Example protocol	23
1.7	A simple authentication protocol	27
1.8	Another simple authentication protocol	28
1.9	STS protocol	31
1.10	STS protocol modified to include identifiers	32
1.11	Key transport protocol providing forward secrecy	34
1.12	Server-based protocol providing forward secrecy	34
1.13	A protocol with weak forward secrecy (MTI protocol)	35
1.14	Protocol of Jiang and Safavi-Naini [400]	39
1.15	Protocol of ntor of Goldberg, Stebila and Ustaoglu [308]	41
3.1	Bird <i>et al.</i> canonical protocol 1	97
3.2	Bellare–Rogaway MAP1 protocol	98
3.3	Protocol for attacking MAP1 protocol	98
3.4	ISO/IEC 9798-2 one-pass unilateral authentication protocol	99
3.5	ISO/IEC 9798-2 two-pass unilateral authentication protocol	99
3.6	ISO/IEC 9798-2 two-pass mutual authentication protocol	100
3.7	ISO/IEC 9798-2 three-pass mutual authentication protocol	101
3.8	ISO/IEC 9798-4 one-pass unilateral authentication protocol	101
3.9	ISO/IEC 9798-4 two-pass unilateral authentication protocol	101
3.10	ISO/IEC 9798-4 two-pass mutual authentication protocol	102
3.11	ISO/IEC 9798-4 three-pass mutual authentication protocol	102
3.12	Woo–Lam unilateral authentication protocol	103
3.13	Andrew secure RPC protocol	105
3.14	Revised Andrew protocol of Burrows <i>et al.</i>	106
3.15	Janson–Tsudik 2PKDP protocol	107
3.16	Boyd two-pass protocol	107

3.17	ISO/IEC 11770-2 Key Establishment Mechanism 1	108
3.18	ISO/IEC 11770-2 Key Establishment Mechanism 2	108
3.19	ISO/IEC 11770-2 Key Establishment Mechanism 3	108
3.20	ISO/IEC 11770-2 Key Establishment Mechanism 4	109
3.21	ISO/IEC 11770-2 Key Establishment Mechanism 5	109
3.22	ISO/IEC 11770-2 Key Establishment Mechanism 6	109
3.23	Needham–Schroeder shared key protocol	111
3.24	Denning–Sacco protocol	112
3.25	Bauer–Berson–Feiertag protocol	112
3.26	Otway–Rees protocol	113
3.27	Otway–Rees protocol modified by Burrows <i>et al.</i>	114
3.28	Otway–Rees protocol modified by Abadi and Needham	115
3.29	Basic Kerberos protocol	116
3.30	Optional Kerberos message to complete mutual authentication	117
3.31	ISO/IEC 11770-2 Key Establishment Mechanism 10	118
3.32	ISO/IEC 11770-2 Key Establishment Mechanism 8	118
3.33	ISO/IEC 11770-2 (1998) Key Establishment Mechanism 12	119
3.34	Key Establishment Mechanism 12 modified by Cheng and Comley	120
3.35	ISO/IEC 11770-2 Key Establishment Mechanism 13	121
3.36	Wide-mouthed-frog protocol	122
3.37	Yahalom protocol	123
3.38	Yahalom protocol modified by Burrows <i>et al.</i>	123
3.39	Janson–Tsudik 3PKDP protocol	125
3.40	Janson–Tsudik optimised 3PKDP protocol	126
3.41	Bellare–Rogaway 3PKD protocol	126
3.42	Woo–Lam key transport protocol	127
3.43	Gong’s timestamp-based protocol	127
3.44	Gong’s nonce-based protocol	128
3.45	Gong’s alternative protocol	128
3.46	Boyd key agreement protocol	129
3.47	Gong’s hybrid protocol	129
3.48	Saha–RoyChowdhury protocol	130
3.49	Gong’s simplified multi-server protocol	132
3.50	Chen–Gollmann–Mitchell multi-server protocol	133
4.1	ISO/IEC 9798-3 one-pass unilateral authentication	138
4.2	ISO/IEC 9798-3 two-pass unilateral authentication	139
4.3	ISO/IEC 9798-3 two-pass mutual authentication	139
4.4	ISO/IEC 9798-3 two-pass mutual authentication with text fields included	139
4.5	ISO/IEC 9798-3 three-pass mutual authentication	140
4.6	Early version of ISO/IEC 9798-3 three-pass mutual authentication	141
4.7	ISO/IEC 9798-3 two-pass parallel authentication	141
4.8	SPLICE/AS protocol	142
4.9	Clark–Jacob variant of SPLICE/AS	143
4.10	Gray variant of SPLICE/AS	143

4.11	ISO/IEC 11770-3 Key Transport Mechanism 1	145
4.12	ISO/IEC 11770-3 Key Transport Mechanism 2	145
4.13	ISO/IEC 11770-3 Key Transport Mechanism 3	146
4.14	Denning–Sacco public key protocol	146
4.15	ISO/IEC 11770-3 Key Transport Mechanism 4	147
4.16	ISO/IEC 11770-3 Key Transport Mechanism 5	147
4.17	ISO/IEC 11770-3 Key Transport Mechanism 6	148
4.18	Helsinki protocol	148
4.19	Blake–Wilson–Menezes key transport protocol	149
4.20	Needham–Schroeder public key protocol	150
4.21	Lowe’s variant of Needham–Schroeder public key protocol	151
4.22	Needham–Schroeder–Lowe protocol modified by Basin <i>et al.</i>	152
4.23	Needham–Schroeder public key protocol using key server	152
4.24	X.509 one-pass authentication	154
4.25	Basin–Cremers–Horvat variant of X.509 one-pass authentication	154
4.26	X.509 two-pass authentication	154
4.27	X.509 three-pass authentication	155
4.28	Ticket granting protocol of public key Kerberos	155
4.29	Basic MSR protocol of Beller, Chang and Yacobi	157
4.30	Improved IMSR protocol of Carlsen	158
4.31	Beller–Yacobi protocol	159
4.32	Improved Beller–Yacobi protocol	160
4.33	Carlsen’s improved Beller–Chang–Yacobi MSR+DH protocol	160
4.34	Simplified TMN protocol (KDP2)	161
4.35	AKA protocol	162
5.1	Diffie–Hellman key agreement	170
5.2	Agnew–Mullin–Vanstone protocol	174
5.3	Original Nyberg–Rueppel protocol	174
5.4	Revised Nyberg–Rueppel protocol	175
5.5	Lim–Lee protocol using static Diffie–Hellman	176
5.6	MTI A(0) protocol	177
5.7	MTI A(k) protocol	177
5.8	Modified MTI B(0) protocol	180
5.9	KEA protocol	187
5.10	Ateniese–Steiner–Tsudik key agreement	188
5.11	Just–Vaudenay–Song–Kim protocol	189
5.12	Unified Model key agreement protocol	190
5.13	MQV protocol	191
5.14	HMQV protocol	193
5.15	NAXOS protocol	197
5.16	CMQV protocol	199
5.17	NETS protocol	200
5.18	SMEN protocol	201
5.19	Protocol of Kim, Fujioka, and Ustaoglu (KFU)	201
5.20	OAKE protocol	203

5.21	Okamoto protocol	204
5.22	Generic addition of key confirmation to basic Diffie–Hellman protocols	205
5.23	Bergsma–Jager–Schwenk protocol instantiated with Diffie–Hellman	209
5.24	STS protocol of Diffie, van Oorschot and Wiener	210
5.25	Modified STS protocol	211
5.26	STS protocol using MACs	211
5.27	Oakley aggressive-mode protocol	213
5.28	Alternative Oakley protocol	214
5.29	Oakley conservative protocol	215
5.30	SKEME protocol, basic mode	217
5.31	IKE main protocol using digital signatures	219
5.32	SIGMA-I protocol	221
5.33	IKEv2 protocol, initial exchanges	223
5.34	JFKi protocol	224
5.35	Arazi’s key agreement protocol	225
5.36	Lim–Lee Schnorr-based protocol	227
5.37	Lim–Lee Schnorr-based variant	227
5.38	Hirose–Yoshida key agreement protocol	228
5.39	Jeong–Katz–Lee protocol TS3	229
5.40	YAK protocol	230
5.41	DIKE protocol	231
5.42	SKEME protocol without forward secrecy	236
5.43	Protocol of Boyd, Cliff, González-Nieto and Paterson	237
5.44	Protocol of Fujioka, Suzuki, Xagawa and Yoneyama	238
5.45	Alawatugoda key agreement protocol	240
6.1	TLS ≤ 1.2 handshake protocol – full handshake	245
6.2	TLS ≤ 1.2 handshake protocol – abbreviated handshake	246
6.3	TLS 1.3 handshake protocol – full handshake	287
6.4	TLS 1.3 handshake protocol – pre-shared key handshake with early application data (‘zero-round-trip’)	288
7.1	Okamoto’s identity-based protocol	295
7.2	Okamoto–Tanaka identity-based protocol	297
7.3	Günther’s key agreement protocol	298
7.4	Günther’s extended key agreement protocol	298
7.5	Saeednia’s variant of Günther’s key agreement protocol	300
7.6	Fiore–Gennaro key agreement protocol	300
7.7	Smart’s identity-based key agreement protocol	304
7.8	Ryu–Yoon–Yoo protocol	306
7.9	Shim’s protocol	307
7.10	Scott’s protocol	308
7.11	Chen–Kudla protocol	309
7.12	Wang’s protocol	310
7.13	Chow and Choo’s protocol	311
7.14	McCullagh–Barreto protocol	312

7.15	Modified McCullagh–Barreto protocol of Cheng and Chen	313
7.16	Boyd–Mao–Paterson protocol	315
7.17	Protocol of Choi, Hwang, Lee and Seo	316
7.18	Protocol of Tian, Susilo, Ming and Wang	318
7.19	Schridde <i>et al.</i> cross-domain identity-based protocol	321
7.20	Girault’s identity-based protocol, adapted by Rueppel and van Oorschot	323
7.21	Protocol of Gorantla, Boyd, and González-Nieto	326
8.1	Diffie–Hellman-based EKE protocol	333
8.2	Augmented Diffie–Hellman-based EKE protocol	336
8.3	PAK protocol	338
8.4	PPK protocol	339
8.5	SPEKE protocol	341
8.6	Dragonfly protocol	343
8.7	SPAKE protocol	344
8.8	J-PAKE protocol	345
8.9	J-PAKE variant of Lancrenon, Škrobot and Tang	346
8.10	Katz–Ostrovsky–Yung protocol	348
8.11	Jiang–Gong protocol	349
8.12	KV-SPOKE protocol of Abdalla, Benhamouda and Pointcheval	351
8.13	Kwon–Song basic protocol	352
8.14	Halevi–Krawczyk password-based protocol	353
8.15	PAK-Z+ protocol	358
8.16	B-SPEKE protocol	359
8.17	SRP protocol	360
8.18	SRP-6 protocol	361
8.19	AMP protocol	362
8.20	AugPAKE	363
8.21	SNAPI protocol	368
8.22	GLNS secret public key protocol	370
8.23	Simplified GLNS secret public key protocol	372
8.24	Optimal GLNS secret public key protocol	373
8.25	Steiner, Tsudik and Waidner three-party EKE	374
8.26	GLNS compact protocol	375
8.27	Optimal GLNS nonce-based protocol	376
8.28	Yen–Liu protocol	376
8.29	Abdalla–Fouque–Pointcheval compiler for three-party PAKE	378
8.30	Wang–Hu compiler for three-party PAKE	380
8.31	Yoneyama protocol for three-party PAKE	381
8.32	Chen–Lim–Yang generic cross-realm PAKE	382
8.33	Abdalla–Bresson–Chevassut–Pointcheval password-based group key exchange	385
9.1	Ingemarsson–Tang–Wong generalised Diffie–Hellman protocol	396
9.2	Steiner–Tsudik–Waidner GDH.1 protocol	397
9.3	Steiner–Tsudik–Waidner GDH.2 protocol	398

9.4	Steiner–Tsudik–Waidner GDH.3 protocol	399
9.5	Steer–Strawczynski–Diffie–Wiener generalised Diffie–Hellman protocol	400
9.6	Kim–Perrig–Tsudik tree Diffie–Hellman protocol	402
9.7	Bresson–Manulis tree Diffie–Hellman protocol	403
9.8	Basic Octopus protocol with four principals	404
9.9	Burmester–Desmedt generalised Diffie–Hellman protocol with broadcasts	405
9.10	Burmester–Desmedt pairwise generalised Diffie–Hellman protocol . .	406
9.11	Ateniese–Steiner–Tsudik A-GDH.2 protocol	413
9.12	Protocol 9.11 when $m = 4$	414
9.13	Ateniese–Steiner–Tsudik SA-GDH.2 protocol	415
9.14	Bresson and Manulis authenticated tree Diffie–Hellman protocol . . .	417
9.15	Bohli–Gonzalez Vasco–Steinwandt protocol	419
9.16	Optimised Bohli–Gonzalez Vasco–Steinwandt protocol of Gao, Neupane and Steinwandt	421
9.17	Manulis–Suzuki–Ustaoglu authenticated Joux protocol	422
9.18	Koyama–Ohta type 1 identity-based group key agreement protocol . .	425
9.19	Saeednia–Safavi-Naini identity-based group key agreement protocol .	428
9.20	Tzeng and Tzeng’s group key agreement protocol	431
9.21	Boyd–González Nieto group key agreement protocol	432
9.22	Burmester–Desmedt star protocol	435
9.23	Hirose–Yoshida group key transport protocol	436
9.24	Mayer–Yung group key transport protocol	438
B.1	First protocol attempt in conventional notation	451

List of Attacks

1.1	Reflection attack on Protocol 1.3	17
1.2	Typing attack on Otway–Rees protocol	19
1.3	Certificate manipulation attack on MTI protocol	21
1.4	Attack on Protocol 1.6	23
1.5	An attack on Protocol 1.7	27
1.6	Lowe’s attack on Protocol 1.10	32
3.1	An oracle attack on Protocol 3.1	97
3.2	Chosen protocol attack on MAP1	99
3.3	Attack on Protocol 3.6	100
3.4	Abadi’s attack on Protocol 3.12	103
3.5	Clark–Jacob attack on Andrew protocol	105
3.6	Lowe’s attack on revised Andrew protocol	106
3.7	Chevalier–Vigneron attack on Denning–Sacco protocol	112
3.8	Buchholtz’s attack on Bauer–Berson–Feiertag protocol	113
3.9	Attack on Otway–Rees protocol without plaintext checking	114
3.10	Attack on Otway–Rees protocol modified by Burrows <i>et al.</i>	115
3.11	Chen–Mitchell attack on ISO/IEC 11770-2 Key Establishment Mechanism 8	118
3.12	Replay attack on Protocol 3.33	120
3.13	Typing attack on Protocol 3.33	120
3.14	Attack on Cheng and Comley’s Protocol 3.34	121
3.15	Attack on wide-mouthed-frog protocol	122
3.16	Syverson’s attack on modified Yahalom protocol	124
3.17	Syverson’s alternative attack on modified Yahalom protocol	124
3.18	Insider attack on Protocol 3.47	130
4.1	Chen–Mitchell attack on Protocol 4.4	140
4.2	Canadian attack on Protocol 4.6	141
4.3	Attack of Clark and Jacob on SPLICE/AS protocol	143
4.4	Attack on Helsinki protocol	148
4.5	Lowe’s attack on Needham–Schroeder public key protocol	150
4.6	Bana–Adão–Sakurada attack on Needham–Schroeder–Lowe protocol	151

4.7	Key compromise impersonation attack on Needham–Schroeder–Lowe protocol	152
4.8	Meadows’ attack on NSPK-KS	153
4.9	Attack of Cervesato <i>et al.</i> on public-key Kerberos	156
4.10	Attack on Beller–Yacobi protocol	159
4.11	Abadi’s attack on AKA protocol	162
5.1	Man-in-the-middle attack on basic Diffie–Hellman	171
5.2	Small subgroup attack on MTI C(1)	179
5.3	Unknown key-share attack on MTI B(0)	180
5.4	Lim–Lee attack on MTI A(0)	181
5.5	Just–Vaudenay impersonation attack on MTI A(0)	182
5.6	Key compromise impersonation attack on MTI C(0)	185
5.7	Unknown key-share attack on generic protocol	186
5.8	Key compromise impersonation attack on Just–Vaudenay–Song–Kim protocol	189
5.9	Kaliski’s unknown key-share attack on MQV protocol	192
6.1	Ray and Dispensa’s attack on TLS renegotiation	275
7.1	Sun and Hsieh’s attack on Shim’s protocol	307
8.1	Ding and Horster’s attack on Protocol 8.25	374
8.2	Lin–Sun–Hwang attack on Protocol 8.25	374
8.3	Attack on Protocol 8.28	377