
Contents

List of Protocols	XVII
List of Attacks	XXIII
1 A Tutorial Introduction to Authentication and Key Establishment	1
1.1 Introduction	1
1.2 Building a Key Establishment Protocol	2
1.2.1 Confidentiality	4
1.2.2 Authentication	5
1.2.3 Replay	8
1.3 Protocol Architectures	12
1.3.1 Existing Cryptographic Keys	12
1.3.2 Method of Session Key Generation	13
1.3.3 Number of Users	13
1.3.4 Example	13
1.4 Cryptographic Properties	14
1.4.1 Confidentiality	16
1.4.2 Data Origin Authentication and Data Integrity	17
1.4.3 Non-repudiation	18
1.4.4 Examples of Cryptographic Algorithms	19
1.4.5 Secret Sharing	20
1.5 Freshness	21
1.6 Types of Attack on Protocols	23
1.6.1 Eavesdropping	24
1.6.2 Modification	25
1.6.3 Replay	25
1.6.4 Preplay	25
1.6.5 Reflection	25
1.6.6 Denial of Service	27
1.6.7 Typing Attacks	28
1.6.8 Cryptanalysis	29

1.6.9	Certificate Manipulation	30
1.6.10	Protocol Interaction	31
1.7	Design Principles for Cryptographic Protocols	31
2	Goals for Authentication and Key Establishment	33
2.1	Introduction	33
2.2	Basic Goals	35
2.2.1	Models of Security	35
2.2.2	Key Establishment or Authentication?	36
2.2.3	User-Oriented Goals	38
2.2.4	Key-Oriented Goals	40
2.3	Enhanced Goals	41
2.3.1	A Hierarchy of Protocol Goals	41
2.3.2	Example: STS Protocol	44
2.3.3	Intensional and Extensional Goals	46
2.3.4	Protocol Efficiency	47
2.3.5	Responsibility and Credit	48
2.4	Goals Concerning Compromised Keys	49
2.4.1	Forward Secrecy	50
2.4.2	Key Compromise Impersonation	52
2.5	Formal Verification of Protocols	52
2.5.1	FDR	53
2.5.2	Mur ϕ	56
2.5.3	Brutus	57
2.5.4	NRL Analyzer	58
2.5.5	BAN Logic	59
2.5.6	Strand Space Model	62
2.5.7	The Inductive Model	63
2.5.8	Comparison of Formal Methods Approaches	65
2.6	Complexity-Theoretic Proofs of Security	66
2.6.1	Model of Communication	67
2.6.2	Defining Security	68
2.6.3	Shoup's Simulation Model	69
2.6.4	A Modular Approach to Proofs	71
2.7	Conclusion	71
3	Protocols Using Shared Key Cryptography	73
3.1	Introduction	73
3.2	Entity Authentication Protocols	75
3.2.1	Bird–Gopal–Herzberg–Janson–Kutten–Molva–Yung Protocols	75
3.2.2	Bellare–Rogaway MAP1 Protocol	76
3.2.3	ISO/IEC 9798-2 Protocols	77
3.2.4	Woo–Lam Authentication Protocol	78
3.2.5	Comparison of Entity Authentication Protocols	80

3.3	Server-Less Key Establishment	80
3.3.1	Andrew Secure RPC Protocol	81
3.3.2	Janson–Tsudik 2PKDP Protocol	83
3.3.3	Boyd Two-Pass Protocol	83
3.3.4	ISO/IEC 11770-2 Server-Less Protocols	84
3.3.5	Comparison of Server-Less Protocols	86
3.4	Server-Based Key Establishment	87
3.4.1	Needham–Schroeder Shared Key Protocol	87
3.4.2	Otway–Rees Protocol	88
3.4.3	Kerberos Protocol	91
3.4.4	ISO/IEC 11770-2 Server-Based Protocols	93
3.4.5	Wide-Mouthed-Frog Protocol	94
3.4.6	Yahalom Protocol	95
3.4.7	Janson–Tsudik 3PKDP Protocol	97
3.4.8	Bellare–Rogaway 3PKD Protocol	98
3.4.9	Woo–Lam Key Transport Protocol	99
3.4.10	Gong Key Agreement Protocols	100
3.4.11	Boyd Key Agreement Protocol	101
3.4.12	Gong Hybrid Protocol	102
3.4.13	Comparison of Server-Based Protocols	103
3.5	Key Establishment Using Multiple Servers	104
3.5.1	Gong’s Multiple Server Protocol	104
3.5.2	Chen–Gollmann–Mitchell Protocol	105
3.6	Conclusion	106
4	Authentication and Key Transport Using Public Key Cryptography	107
4.1	Introduction	107
4.1.1	Notation	108
4.1.2	Design Principles for Public Key Protocols	108
4.2	Entity Authentication Protocols	110
4.2.1	Protocols in ISO/IEC 9798-3	110
4.2.2	Protocols in ISO/IEC 9798-5	113
4.2.3	SPLICE/AS	113
4.2.4	Comparison of Entity Authentication Protocols	115
4.3	Key Transport Protocols	116
4.3.1	Protocols in ISO/IEC 11770-3	116
4.3.2	Blake-Wilson and Menezes Provably Secure Key Transport Protocol	120
4.3.3	Needham–Schroeder Public Key Protocol	121
4.3.4	Protocols in the X.509 Standard	122
4.3.5	TLS Protocol	124
4.3.6	Beller–Chang–Yacobi Protocols	126
4.3.7	TMN Protocol	131
4.3.8	AKA Protocol	132

4.3.9	Comparison of Key Transport Protocols	133
4.4	Conclusion	134
5	Key Agreement Protocols	137
5.1	Introduction	137
5.1.1	Key Control	138
5.1.2	Unknown Key-Share Attacks	139
5.1.3	Classes of Key Agreement	140
5.2	Diffie–Hellman Key Agreement	141
5.2.1	Small Subgroup Attacks	144
5.2.2	ElGamal Encryption and One-Pass Key Establishment	144
5.2.3	Lim–Lee Protocol Using Static Diffie–Hellman	146
5.3	MTI Protocols	147
5.3.1	Small Subgroup Attack on MTI Protocols	149
5.3.2	Unknown Key-Share Attacks on MTI Protocols	150
5.3.3	Lim–Lee Attack on MTI Protocols	151
5.3.4	Impersonation Attack of Just and Vaudenay	152
5.3.5	Triangle Attacks on MTI Protocols	153
5.3.6	Forward Secrecy and Key Compromise Impersonation for MTI Protocols	154
5.4	Diffie–Hellman-Based Protocols with Basic Message Format	155
5.4.1	The Goss Protocol	156
5.4.2	KEA Protocol	157
5.4.3	The Unified Model Protocol	158
5.4.4	MQV Protocol	159
5.4.5	Yacobi’s Protocol	160
5.4.6	Ateniese–Steiner–Tsudik Protocol	161
5.4.7	Just–Vaudenay–Song–Kim Protocol	162
5.4.8	Adding Key Confirmation	163
5.4.9	Comparison	164
5.5	Diffie–Hellman-Based Protocols with Enhanced Message Format	165
5.5.1	STS Protocol	166
5.5.2	Oakley Protocol	168
5.5.3	SKEME Protocol	172
5.5.4	Internet Key Exchange	174
5.5.5	Arazi’s Protocol	178
5.5.6	Lim–Lee Protocols	179
5.5.7	Hirose–Yoshida Protocol	180
5.5.8	Comparison	181
5.6	Identity-Based Schemes	182
5.6.1	Okamoto’s Scheme	184
5.6.2	Günther’s Scheme	186
5.6.3	Girault’s Scheme	188
5.6.4	Schemes Using Signatures with Message Recovery	190

5.7	Protocols Designed for Computationally Limited Devices	190
5.7.1	Yacobi–Shmueli Protocol	191
5.7.2	ASPeCT Protocol	192
5.7.3	Jakobsson–Pointcheval Protocol	193
5.8	Protocols in ISO/IEC 11770-3	195
5.9	Diffie–Hellman Key Agreement in Other Groups	196
5.10	Protocols Not Based on Diffie–Hellman	197
5.10.1	SKEME without Forward Secrecy	197
5.10.2	Key Pre-distribution Schemes	198
5.11	Conclusion	199
6	Conference Key Protocols	201
6.1	Introduction	201
6.1.1	Generalised Security Goals	202
6.1.2	Static and Dynamic Groups	203
6.1.3	Notation	204
6.2	Generalising Diffie–Hellman Key Agreement	204
6.2.1	Ingemarsson–Tang–Wong Key Agreement	204
6.2.2	Steiner–Tsudik–Waidner Key Agreement	206
6.2.3	Steer–Strawczynski–Diffie–Wiener Key Agreement	209
6.2.4	Perrig’s Generalised Diffie–Hellman	210
6.2.5	Becker and Wille’s Octopus Protocol	212
6.2.6	Burmester–Desmedt Key Agreement	214
6.2.7	Joux’s Tripartite Diffie–Hellman	215
6.2.8	Security of Generalised Diffie–Hellman	216
6.2.9	Efficiency of Generalised Diffie–Hellman	217
6.3	Conference Key Agreement Protocols	219
6.3.1	Authenticating Generalised Diffie–Hellman	219
6.3.2	Klein–Ottens–Beth Protocol	220
6.3.3	Authenticated GDH Protocols	221
6.4	Identity-Based Conference Key Protocols	225
6.4.1	Koyama and Ohta Protocols	226
6.4.2	Protocols of Saeednia and Safavi-Naini	229
6.5	Conference Key Agreement without Diffie–Hellman	230
6.5.1	Pieprzyk and Li’s Key Agreement Protocol	230
6.5.2	Tzeng–Tzeng Protocols	232
6.5.3	Boyd’s Conference Key Agreement	233
6.6	Conference Key Transport Protocols	235
6.6.1	Burmester–Desmedt Star and Tree Protocols	235
6.6.2	Mayer and Yung’s Protocols	237
6.6.3	Key Hierarchies	239
6.7	Key Broadcasting Protocols	240
6.7.1	Key Broadcasting Using Number Theory	242
6.7.2	Key Broadcasting Using Secret Sharing	244
6.8	Conclusion	245

7	Password-Based Protocols	247
7.1	Introduction	247
7.2	Encrypted Key Exchange Using Diffie–Hellman	250
7.2.1	Bellovin–Merritt’s Original EKE	250
7.2.2	The PAK Protocol	252
7.2.3	SPEKE	256
7.2.4	Katz–Ostrovsky–Yung Protocol	258
7.3	Augmented EKE	260
7.3.1	B-SPEKE	263
7.3.2	SRP Protocol	264
7.3.3	AMP Protocol	265
7.4	Three-Party EKE	266
7.4.1	GLNS Secret Public Key Protocols	267
7.4.2	Steiner, Tsudik and Waidner Three-Party EKE	271
7.5	RSA-Based Protocols	273
7.5.1	RSA-Based EKE	273
7.5.2	OKE and SNAP1	274
7.6	Protocols Using a Server Public Key	276
7.6.1	GLNS Protocols with Server Public Keys	277
7.6.2	Kwon–Song Protocols	278
7.6.3	Halevi–Krawczyk Protocols	279
7.6.4	Three-Party Protocol of Yen and Liu	280
7.7	Other Protocols	282
7.7.1	Lee–Sohn–Yang–Won Protocol	282
7.7.2	Anderson–Lomas Protocol	283
7.7.3	Strengthening Passwords	284
7.8	Conclusion	285
A	Standards for Authentication and Key Establishment	289
A.1	ISO Standards	289
A.1.1	ISO/IEC 9798	289
A.1.2	ISO/IEC 11770	290
A.1.3	ISO 9594-8/ITU X.509	290
A.2	Other Standards	290
A.2.1	IETF Standards	290
A.2.2	IEEE P1363-2000	291
A.2.3	NIST and ANSI Standards	291
B	Summary of Notation	293
	References	295
	Index of Protocols	317
	General Index	319