
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	2.7.1	Models for Group Key Exchange	86
1.5.3	Entity Authentication	26	2.7.2	Models for Multi-factor Key Exchange	87
1.5.4	Key Establishment	28	2.8	Secure Channels	88
1.5.5	Key Confirmation	29	2.8.1	CK01 Secure Channels	89
1.5.6	Example: STS Protocol	31	2.8.2	CK02 Secure Channels	91
1.5.7	Forward Secrecy	33	2.8.3	Authenticated and Confidential Channel Establishment (ACCE) Protocols	91
1.5.8	Weak Forward Secrecy	35	2.9	Conclusion	93
1.5.9	Key Compromise Impersonation	36			
1.5.10	Deniability	37			
1.5.11	Anonymity	39	3	Protocols Using Shared Key Cryptography	95
1.5.12	Protocol Efficiency	41	3.1	Introduction	95
1.6	Tools for Verification of Protocols	43	3.2	Entity Authentication Protocols	96
1.6.1	FDR	44	3.2.1	Bird-Gopal-Herzberg-Janson-Kutten-Molva-Yung Protocols	97
1.6.2	NRL Analyzer and Maude-NPA	47	3.2.2	Bellare-Rogaway MAP1 Protocol	98
1.6.3	ProVerif	48	3.2.3	ISO/IEC 9798-2 Protocols	99
1.6.4	Scyther and Tamarin	48	3.2.4	ISO/IEC 9798-4 Protocols	101
1.6.5	Tools for Computational Models	50	3.2.5	Woo-Lam Authentication Protocol	102
1.6.6	Comparison of Tools	51	3.2.6	Comparison of Entity Authentication Protocols	103
1.7	Conclusion	52	3.3	Server-Less Key Establishment	104
2	Computational Security Models	53	3.3.1	Andrew Secure RPC Protocol	104
2.1	Introduction	53	3.3.2	Janson-Tsudik 2PKDP Protocol	106
2.1.1	The Significance of a Computational Proof of Security	54	3.3.3	Boyd Two-Pass Protocol	107
2.1.2	Elements of Computational Models	55	3.3.4	ISO/IEC 11770-2 Server-Less Protocols	108
2.2	Bellare-Rogaway Model	58	3.3.5	Comparison of Server-Less Protocols	110
2.2.1	BR93: The First Computational Model	58	3.4	Server-Based Key Establishment	110
2.2.2	BR95: Server-Based Protocols	65	3.4.1	Needham-Schroeder Shared Key Protocol	111
2.2.3	The Public Key Setting: The BWM and BWJM Models	66	3.4.2	Otway-Rees Protocol	113
2.2.4	BPR00: Forward Secrecy and Passwords	67	3.4.3	Kerberos Protocol	115
2.2.5	Summarising the BR Model Variants	69	3.4.4	ISO/IEC 11770-2 Server-Based Protocols	117
2.3	Canetti-Krawczyk Model	69	3.4.5	Wide-Mouthed-Frog Protocol	122
2.3.1	BCK98 Model	69	3.4.6	Yahalom Protocol	122
2.3.2	CK01 Model	70	3.4.7	Janson-Tsudik 3PKDP Protocol	125
2.3.3	HMQV Model	75	3.4.8	Bellare-Rogaway 3PKD Protocol	126
2.4	eCK Model	76	3.4.9	Woo-Lam Key Transport Protocol	126
2.4.1	MU08 Model	78	3.4.10	Gong Key Agreement Protocols	127
2.4.2	eCK-PFS Model	78	3.4.11	Boyd Key Agreement Protocol	129
2.4.3	seCK Model	79	3.4.12	Gong Hybrid Protocol	129
2.5	Comparing Computational Models for Key Exchange	79	3.4.13	Comparison of Server-Based Protocols	130
2.5.1	Comparing the BR and CK Models	80	3.5	Key Establishment Using Multiple Servers	132
2.5.2	Comparing eCK and Other Models	81	3.5.1	Gong's Multiple Server Protocol	132
2.5.3	Sessions and Session Identifiers	82	3.5.2	Chen-Gollmann-Mitchell Protocol	133
2.5.4	Incorporating Public Key Infrastructure	83	3.6	Conclusion	134
2.6	Shoup's Simulation Model	84			
2.7	Models for Enhanced Scenarios	85			

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 Morioka-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
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	9.4.1	Koyama and Ohta Protocols	424
8.5.1	RSA-Based EKE	366	9.4.2	Protocols of Saeednia and Safavi-Naini	427
8.5.2	OKE and SNAPI	367	9.4.3	ID-Based Group Key Agreement and Pairings	428
8.6	Three-Party PAKE Protocols	369	9.5	Group Key Agreement without Diffie–Hellman	429
8.6.1	GLNS Secret Public Key Protocols	369	9.5.1	Pieprzyk and Li's Key Agreement Protocol	429
8.6.2	Steiner, Tsudik and Waidner Three-Party EKE	373	9.5.2	Tzeng–Tzeng Protocols	430
8.6.3	GLNS Protocols with Server Public Keys	375	9.5.3	Boyd–González Nieto Group Key Agreement	432
8.6.4	Three-Party Protocol of Yen and Liu	376	9.5.4	Generic One-Round Group Key Agreement from Multi-KEM	433
8.6.5	Generic Protocol of Abdalla, Fouque and Pointcheval	377	9.5.5	Asymmetric Group Key Agreement	434
8.6.6	Stronger Security Models for Three-Party PAKE	378	9.6	Group Key Transport Protocols	434
8.6.7	Three-Party Protocol of Yoneyama	379	9.6.1	Burmester–Desmedt Star and Tree Protocols	434
8.6.8	Cross-Realm PAKE Protocols	380	9.6.2	Mayer and Yung's Protocols	437
8.6.9	Comparing Three-Party PAKE Protocols	383	9.6.3	Key Hierarchies	439
8.7	Group PAKE Protocols	383	9.7	Conclusion	440
8.7.1	Concrete Protocol Constructions	384			
8.7.2	Generic Constructions	386	A	Standards for Authentication and Key Establishment	441
8.8	Conclusion	387	A.1	ISO Standards	441
9	Group Key Establishment	389	A.1.1	ISO/IEC 9798	441
9.1	Introduction	389	A.1.2	ISO/IEC 11770	442
9.1.1	Efficiency in Group Key Establishment	390	A.1.3	ISO 9594-8/ITU X.509	443
9.1.2	Generalised Security Goals	390	A.2	IETF Standards	443
9.1.3	Static and Dynamic Groups	392	A.3	IEEE P1363 Standards	444
9.1.4	Insider Attacks	393	A.4	NIST Standards	444
9.1.5	Notation	394	A.5	Other Standards and Protocols	446
9.2	Generalising Diffie–Hellman Key Agreement	394	A.5.1	ANSI	446
9.2.1	Ingemarsson–Tang–Wong Key Agreement	395	A.5.2	Widely Deployed Protocols	447
9.2.2	Steiner–Tsudik–Waidner Key Agreement	396	B	Tutorial: Building a Key Establishment Protocol	449
9.2.3	Steer–Strawczynski–Diffie–Wiener Key Agreement	399	B.1	Confidentiality	451
9.2.4	Kim–Perrig–Tsudik Tree Diffie–Hellman	400	B.2	Authentication	453
9.2.5	Becker and Wille's Octopus Protocol	402	B.3	Replay	455
9.2.6	Burmester–Desmedt Key Agreement	404	B.4	Design Principles for Cryptographic Protocols	459
9.2.7	One-Round Tripartite and Multi-Party Diffie–Hellman	407	C	Summary of Notation	461
9.2.8	Security of Generalised Diffie–Hellman	407			
9.2.9	Efficiency of Generalised Diffie–Hellman	408	References	463	
9.3	Group Key Agreement Protocols	410	General Index	513	
9.3.1	Authenticating Generalised Diffie–Hellman	410	Protocol Index	519	
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			