

---

## List of Protocols

1.1	First protocol attempt in conventional notation	3
1.2	A protocol in an unusual class	14
1.3	Use of a nonce (random challenge)	22
1.4	A protocol vulnerable to reflection attack	26
1.5	Otway–Rees protocol	28
1.6	A protocol vulnerable to certificate manipulation (MTI protocol)	30
2.1	Example protocol	34
2.2	A simple authentication protocol	38
2.3	Another simple authentication protocol	39
2.4	STS protocol	44
2.5	STS protocol modified to include identifiers	45
2.6	A protocol in which <i>A</i> takes ‘responsibility’	49
2.7	A protocol in which <i>A</i> takes ‘credit’	49
2.8	Key transport protocol providing forward secrecy	51
2.9	Server-based protocol providing forward secrecy	51
3.1	Bird <i>et al.</i> canonical protocol 1	75
3.2	Bellare–Rogaway MAP1 protocol	76
3.3	Protocol for attacking MAP1 protocol	76
3.4	ISO/IEC 9798-2 one-pass unilateral authentication protocol	77
3.5	ISO/IEC 9798-2 two-pass unilateral authentication protocol	78
3.6	ISO/IEC 9798-2 two-pass mutual authentication protocol	78
3.7	ISO/IEC 9798-2 three-pass mutual authentication protocol	78
3.8	Woo–Lam unilateral authentication protocol	79
3.9	Andrew secure RPC protocol	81
3.10	Revised Andrew protocol of Burrows <i>et al.</i>	82
3.11	Janson–Tsudik 2PKDP protocol	83
3.12	Boyd two-pass protocol	84
3.13	ISO/IEC 11770-2 Key Establishment Mechanism 1	84
3.14	ISO/IEC 11770-2 Key Establishment Mechanism 2	84
3.15	ISO/IEC 11770-2 Key Establishment Mechanism 3	85
3.16	ISO/IEC 11770-2 Key Establishment Mechanism 4	85

XVIII List of Protocols

3.17	ISO/IEC 11770-2 Key Establishment Mechanism 5	85
3.18	ISO/IEC 11770-2 Key Establishment Mechanism 6	86
3.19	Needham–Schroeder shared key protocol	88
3.20	Denning–Sacco protocol	88
3.21	Bauer–Berson–Feiertag protocol	88
3.22	Otway–Rees protocol	89
3.23	Otway–Rees protocol modified by Burrows <i>et al.</i>	90
3.24	Otway–Rees protocol modified by Abadi and Needham	91
3.25	Basic Kerberos protocol	92
3.26	Optional Kerberos message to complete mutual authentication	92
3.27	ISO/IEC 11770-2 Key Establishment Mechanism 10	93
3.28	ISO/IEC 11770-2 Key Establishment Mechanism 12	94
3.29	ISO/IEC 11770-2 Key Establishment Mechanism 13	94
3.30	Wide-mouthed-frog protocol	94
3.31	Yahalom protocol	95
3.32	Yahalom protocol modified by Burrows <i>et al.</i>	96
3.33	Janson–Tsudik 3PKDP protocol	98
3.34	Janson–Tsudik optimised 3PKDP protocol	98
3.35	Bellare–Rogaway 3PKD protocol	99
3.36	Woo–Lam key transport protocol	99
3.37	Gong’s timestamp-based protocol	100
3.38	Gong’s nonce-based protocol	100
3.39	Alternative Gong’s protocol	101
3.40	Boyd key agreement protocol	101
3.41	Gong’s hybrid protocol	102
3.42	Gong’s simplified multi-server protocol	104
3.43	Chen–Gollmann–Mitchell multi-server protocol	105
4.1	ISO/IEC 9798-3 one-pass unilateral authentication	110
4.2	ISO/IEC 9798-3 two-pass unilateral authentication	111
4.3	ISO/IEC 9798-3 two-pass mutual authentication	111
4.4	ISO/IEC 9798-3 three-pass mutual authentication	112
4.5	Early version of ISO/IEC 9798-3 three-pass mutual authentication	112
4.6	ISO/IEC 9798-3 two-pass parallel authentication	113
4.7	SPLICE/AS protocol	114
4.8	Clark–Jacob variant of SPLICE/AS	114
4.9	Gray variant of SPLICE/AS	115
4.10	ISO/IEC 11770-3 Key Transport Mechanism 1	116
4.11	ISO/IEC 11770-3 Key Transport Mechanism 2	117
4.12	ISO/IEC 11770-3 Key Transport Mechanism 3	118
4.13	Denning–Sacco public key protocol	118
4.14	ISO/IEC 11770-3 Key Transport Mechanism 4	118
4.15	ISO/IEC 11770-3 Key Transport Mechanism 5	119
4.16	ISO/IEC 11770-3 Key Transport Mechanism 6	119
4.17	Helsinki protocol	120

4.18	Blake-Wilson-Menezes provably secure key transport protocol . . .	121
4.19	Needham-Schroeder public key protocol . . . . .	121
4.20	Lowe's variant of Needham-Schroeder public key protocol . . . . .	122
4.21	X.509 one-pass authentication . . . . .	123
4.22	X.509 two-pass authentication . . . . .	123
4.23	X.509 three-pass authentication . . . . .	124
4.24	Simplified TLS key transport protocol . . . . .	125
4.25	Simplified TLS key agreement protocol . . . . .	126
4.26	Basic MSR protocol of Beller, Chang and Yacobi . . . . .	127
4.27	Improved IMSR protocol of Carlsen . . . . .	128
4.28	Beller-Yacobi protocol . . . . .	129
4.29	Improved Beller-Yacobi protocol . . . . .	130
4.30	Carlsen's improved Beller-Chang-Yacobi MSR + DH protocol . . . . .	131
4.31	Simplified TMN protocol (KDP2) . . . . .	132
4.32	AKA protocol . . . . .	132
5.1	Diffie-Hellman key agreement . . . . .	141
5.2	Agnew-Mullin-Vanstone protocol . . . . .	145
5.3	Original Nyberg-Rueppel protocol . . . . .	145
5.4	Revised Nyberg-Rueppel protocol . . . . .	146
5.5	Lim-Lee protocol using static Diffie-Hellman . . . . .	147
5.6	MTI A(0) protocol . . . . .	148
5.7	MTI A(k) protocol . . . . .	148
5.8	Modified MTI B(0) protocol . . . . .	151
5.9	KEA protocol . . . . .	157
5.10	Unified Model key agreement . . . . .	158
5.11	MQV protocol . . . . .	159
5.12	Ateniese-Steiner-Tsudik key agreement . . . . .	161
5.13	Just-Vaudenay-Song-Kim protocol . . . . .	162
5.14	Generic addition of key confirmation to basic DH protocols . . . . .	164
5.15	STS protocol . . . . .	166
5.16	Modified STS protocol . . . . .	167
5.17	STS protocol using MACs . . . . .	168
5.18	Oakley aggressive mode protocol . . . . .	169
5.19	Alternative Oakley protocol . . . . .	170
5.20	Oakley conservative protocol . . . . .	171
5.21	SKEME protocol basic mode . . . . .	173
5.22	IKE main protocol using digital signatures . . . . .	176
5.23	Arazi's key agreement protocol . . . . .	178
5.24	Lim-Lee Schnorr-based protocol . . . . .	179
5.25	Lim-Lee Schnorr-based variant . . . . .	180
5.26	Hirose-Yoshida key agreement protocol . . . . .	181
5.27	Okamoto's identity-based protocol . . . . .	184
5.28	Okamoto-Tanaka identity-based protocol . . . . .	186
5.29	Günther's key agreement protocol . . . . .	187
5.30	Günther's extended key agreement protocol . . . . .	188

5.31	Saeednia's variant of Günther's key agreement protocol	189
5.32	Girault's identity-based protocol	190
5.33	Yacobi–Shmueli protocol	191
5.34	Park key agreement protocol	192
5.35	ASPeCT protocol	193
5.36	Jakobsson–Pointcheval protocol	194
5.37	Wong–Chan protocol	195
5.38	SKEME protocol without forward secrecy	197
6.1	Ingemarsson–Tang–Wong generalised Diffie–Hellman	206
6.2	Steiner–Tsudik–Waidner GDH.1	207
6.3	Steiner–Tsudik–Waidner GDH.2	207
6.4	Steiner–Tsudik–Waidner GDH.3	209
6.5	Steer–Strawczynski–Diffie–Wiener generalised Diffie–Hellman	210
6.6	Perrig's generalised Diffie–Hellman	212
6.7	Four-principal basic Octopus protocol	213
6.8	Burmester–Desmedt generalised Diffie–Hellman with broadcasts	214
6.9	Burmester–Desmedt pairwise generalised Diffie–Hellman	216
6.10	Ateniese–Steiner–Tsudik A-GDH.2	222
6.11	Protocol 6.10 when $m = 4$	223
6.12	Ateniese–Steiner–Tsudik SA-GDH.2	224
6.13	Koyama–Ohta type 1 identity-based conference key agreement	227
6.14	Saeednia–Safavi-Naini identity-based conference key agreement	230
6.15	Tzeng and Tzeng's conference key agreement	233
6.16	Boyd's conference key agreement	234
6.17	Burmester–Desmedt star protocol	236
6.18	Hirose–Yoshida conference key transport protocol	236
6.19	Mayer–Yung conference key transport protocol	238
6.20	Chiou–Chen's key broadcasting	243
6.21	Key broadcasting using secret sharing	244
7.1	Diffie–Hellman-based EKE protocol	250
7.2	PAK protocol	254
7.3	PPK protocol	255
7.4	PAK-R protocol	256
7.5	SPEKE protocol	257
7.6	Katz–Ostrovsky–Yung protocol	259
7.7	Augmented Diffie–Hellman-based EKE protocol	261
7.8	PAK-Y protocol	262
7.9	B-SPEKE protocol	263
7.10	SRP protocol	264
7.11	AMP protocol	266
7.12	GLNS secret public key protocol	267
7.13	Simplified GLNS secret public key protocol	269
7.14	Optimal GLNS secret public key protocol	271
7.15	Steiner, Tsudik and Waidner three-party EKE	271
7.16	SNAPI protocol	275

7.17	GLNS compact protocol	277
7.18	Optimal GLNS nonce-based protocol	278
7.19	Kwon–Song basic protocol	279
7.20	Halevi–Krawczyk password-based protocol	280
7.21	Yen–Liu protocol	281
7.22	Lee–Sohn–Yang–Won protocol	282
7.23	Anderson–Lomas protocol	283



---

## List of Attacks

1.1	Reflection attack on Protocol 1.4	26
1.2	Typing attack on Otway–Rees protocol	29
1.3	Certificate manipulation attack on MTI protocol	30
2.1	Attack on Protocol 2.1	34
2.2	An attack on Protocol 2.2	39
2.3	Lowe’s attack on Protocol 2.5	45
3.1	An oracle attack on Protocol 3.1	76
3.2	Chosen protocol attack on MAP1	77
3.3	Abadi’s attack on Protocol 3.8	79
3.4	Clark–Jacob attack on Andrew protocol	81
3.5	Lowe’s attack on revised Andrew protocol	82
3.6	Attack on Otway–Rees protocol without plaintext checking	89
3.7	Attack on Otway–Rees protocol modified by Burrows <i>et al.</i>	90
3.8	Attack on Wide-mouthed-frog protocol	95
3.9	Syverson’s attack on modified Yahalom protocol	97
3.10	Alternative Syverson’s attack on modified Yahalom protocol	97
3.11	Insider attack on Protocol 3.41	102
4.1	Canadian attack on Protocol 4.5	112
4.2	Attack of Clark–Jacob on SPLICE/AS protocol	114
4.3	Attack on Helsinki protocol	120
4.4	Lowe’s attack on Needham–Schroeder public key protocol	122
4.5	Attack on Beller–Yacobi protocol	130
4.6	Abadi’s attack on AKA protocol	133
5.1	Attack on basic Diffie–Hellman	142
5.2	Small subgroup attack on MTI C(1) protocol	150
5.3	Unknown key-share attack on MTI B(0) protocol	150
5.4	Lim–Lee attack on MTI A(0)	152
5.5	Just–Vaudenay impersonation attack on MTI A(0) protocol	153
5.6	Key compromise impersonation on MTI C(0)	155
5.7	Unknown key-share attack on generic protocol	156
5.8	Kaliski’s unknown key-share attack on MQV protocol	160

XXIV List of Attacks

5.9	Key compromise impersonation on Just–Vaudenay–Song–Kim protocol.....	163
5.10	Attack on Park key agreement .....	192
7.1	Ding and Horster’s attack on Protocol 7.15 .....	272
7.2	Lin–Sun–Hwang attack on Protocol 7.15 .....	272
7.3	Attack on Protocol 7.21 .....	281