

Contents

1	Introduction of Cryptographic Protocols	1
1.1	Information security and cryptography	2
1.2	Classes of cryptographic protocols	3
1.2.1	Authentication protocol	3
1.2.2	Key establishment protocol	4
1.2.3	Electronic commerce protocol	4
1.2.4	Secure multi-party protocol	5
1.3	Security of cryptographic protocols	5
1.4	Motivations of this book	9
	References	11
2	Background of Cryptographic Protocols	13
2.1	Preliminaries	13
2.1.1	Functions	13
2.1.2	Terminology	14
2.2	Cryptographic primitives	16
2.2.1	Cryptology	16
2.2.2	Symmetric-key encryption	18
2.2.3	Public-key encryption	19
2.2.4	Digital signatures	19
2.2.5	Hash Functions	20
2.2.6	Message authentication	21
2.3	Cryptographic protocols	24
2.3.1	Secure channel	25
2.3.2	Principals	26
2.3.3	Time-variant parameters	27
2.3.4	Challenge and response	29
2.3.5	Other classes of cryptographic protocols	29
2.4	Security of cryptographic protocols	30
2.4.1	Attacks on primitives	30
2.4.2	Attacks on protocols	31

2.4.3	Security of protocols	32
2.4.4	Analysis methods for protocol security	35
2.5	Communication threat model	36
2.5.1	Dolev-Yao threat model	36
2.5.2	Assumptions of protocol environment	37
2.5.3	Expressions of cryptographic protocols	40
References		40
3	Engineering Principles for Security Design of Protocols	41
3.1	Introduction of engineering principles	42
3.1.1	Prudent engineering principles	42
3.1.2	Cryptographic protocol engineering principles	43
3.2	Protocol engineering requirement analysis	45
3.2.1	Security requirement analysis	45
3.2.2	Plaintext analysis	46
3.2.3	Application environment analysis	47
3.2.4	Attack model and adversary abilities analysis	48
3.2.5	Cryptographic service requirement analysis	50
3.3	Detailed protocol design	50
3.3.1	Liveness of the principal's identity	51
3.3.2	Freshness and association of time-variant parameter	63
3.3.3	Data integrity protection of message	69
3.3.4	Stepwise refinement	71
3.4	Provable security	76
References		78
4	Informal Analysis Schemes of Cryptographic Protocols	83
4.1	The security of cryptographic protocols	84
4.1.1	Authenticity and confidentiality under computational model	85
4.1.2	Security definitions	86
4.2	Security mechanism based on trusted freshenss	87
4.2.1	Notions	88
4.2.2	Freshness principle	93
4.2.3	Security of authentication protocol	95
4.2.4	Manual analysis based on trusted freshness	96
4.2.5	Application of security analysis based on trusted freshness	98
4.3	Analysis of classic attacks	100
4.3.1	Man in the middle attack	101
4.3.2	Source-substitution attack	103

4.3.3	Message replay attack	107
4.3.4	Parallel session attack	112
4.3.5	Reflection attack	117
4.3.6	Interleaving attack	118
4.3.7	Attack due to type flaw	123
4.3.8	Attack due to name omission	126
4.3.9	Attack due to misuse of cryptographic services	129
4.3.10	Security analysis of other protocols	131
	References	150
5	Security Analysis of Real World Protocols	153
5.1	Secure Socket Layer and Transport Layer Security	154
5.1.1	SSL and TLS overview	155
5.1.2	The SSL handshake protocol	156
5.1.3	Security analysis of SSL based on trusted freshness	162
5.2	Internet Protocol Security	172
5.2.1	IPSec overview	173
5.2.2	Internet Key Exchange	176
5.2.3	Security analysis of IKE based on trusted freshness	184
5.3	Kerberos — the network authentication protocol	193
5.3.1	Kerberos overview	193
5.3.2	Basic Kerberos network authentication service	198
5.3.3	Security analysis of Kerberos based on trusted freshness	200
5.3.4	Public-key Kerberos	204
	References	212
6	Guarantee of Cryptographic Protocol Security	215
6.1	Security definition of authentication	216
6.1.1	Formal modeling of protocols	217
6.1.2	Formal modeling of communications	217
6.1.3	Formal modeling of entity authentication	218
6.2	Security definition of SK-security	221
6.2.1	Protocol and adversary models in CK model	222
6.2.2	SK-security in CK model	225
6.3	Authentication based on trusted freshness	226
6.3.1	Trusted freshness	226
6.3.2	Liveness of principal	230
6.3.3	Confidentiality of freshness identifier	232
6.3.4	Freshness of freshness identifier	232
6.3.5	Association of freshness identifier	233

6.3.6	Security analysis based on trusted freshness	234
6.3.7	Definition of security	236
6.3.8	Non-repudiation based on trusted freshness	242
	References	246
7	Formalism of Protocol Security Analysis	249
7.1	BAN logic	250
7.1.1	Basic notation	251
7.1.2	Logical postulate	252
7.1.3	Steps for security analysis based on BAN logic	253
7.1.4	BAN-like logic	254
7.2	Model checking	255
7.3	Theorem proving	256
7.4	Belief multisets based on trusted freshness	257
7.4.1	Belief logic language	257
7.4.2	Logical postulate	261
7.5	Applications of belief multiset formalism	273
7.5.1	Analysis of Needham-Schroeder public-key protocol	274
7.5.2	Analysis of Kerberos pair-key agreement in DSNs	279
7.5.3	Analysis of authentication in IEEE 802.11i	282
7.6	Comparison	292
	References	295
8	Design of Cryptographic Protocols Based on Trusted Freshness	299
8.1	Previously known methods for protocol design	300
8.1.1	A simple logic for authentication protocol design	300
8.1.2	Fail-stop protocol design	301
8.1.3	Authentication test	301
8.1.4	Canetti-Krawczyk model	302
8.1.5	Models for secure protocol design and their compositions	303
8.2	Security properties to achieve in protocol design	305
8.2.1	Confidentiality	305
8.2.2	Data integrity	306
8.2.3	Data origin authentication	306
8.2.4	Entity authentication	310
8.2.5	Origin entity authentication	314
8.2.6	Non-repudiation	315
8.2.7	Access control	317
8.2.8	Key establishment	318

8.2.9	Fairness	319
8.3	Protocol design based on trusted freshness	320
8.3.1	Notations and descriptions	321
8.3.2	Design of cryptographic protocols	326
8.3.3	Lower bounds for SK-secure protocols	328
8.4	Application of protocol design via trusted freshness	334
8.4.1	Construction of a two-party key establishment protocol	336
	References	339
9	Automated Analysis of Cryptographic Protocols Based on Trusted Freshness	341
9.1	Previously known methods for automated analysis	342
9.1.1	Automated analysis tool based on logic	342
9.1.2	Automated analysis tool based on model checking	343
9.1.3	Automated analysis tool based on theorem proving	346
9.1.4	CAPSL specification language	346
9.2	Automated cryptographic protocol analysis based on trusted freshness	347
9.2.1	Analyzer frame based on belief multiset formalism	347
9.2.2	Comparison of two initial implementations of BMF	349
9.2.3	Implementation of the belief multiset formalism	352
	References	367
	Index	371