

Contents

1	Introduction	1
1.1	Cryptographic Algorithms	1
1.1.1	Symmetric Cryptographic Algorithms	2
1.1.2	Asymmetric Algorithms	3
1.2	Using Cryptographic Algorithms	4
1.2.1	Block Cipher Modes	4
1.2.2	Hash Function	5
1.2.3	Hashed Message Authentication Code	6
1.2.4	Asymmetric Encryption and Signatures	6
1.3	Cryptographic Protocols and Security Protocols	7
1.3.1	Security Protocols	7
1.3.2	Symmetric Protocols	8
1.3.3	Symmetric Security Protocols	9
2	Some Useful Constructions	11
2.1	Hash Chains	11
2.1.1	Hash Accumulator	12
2.1.2	Hash Tree	12
2.2	Random Subsets	15
2.2.1	$\mathcal{S}_i \subset \mathcal{S}^n$	15
2.2.2	$(\mathcal{S}_i \cap \mathcal{S}_j) \subset \mathcal{S}^n$	16
3	Nonscalable Key Distribution Schemes	19
3.1	Online KDC	20
3.1.1	NS Protocol	20
3.1.2	Leighton–Micali Protocol	20
3.2	Offline KDC	22
3.2.1	Basic KDS for Static Small-Scale Networks	22
3.2.2	Key Distribution for Dynamic Networks	23
3.3	MLS Key Distribution	23
3.3.1	Identity Ticket (IT) Scheme	25
3.4	Comparison	26

3.4.1	MLS with Multiple KDCs	27
3.4.2	MLS Applications	28
4	MLS for Internet Security Protocols	31
4.1	Domain Name System	31
4.1.1	DNS Records	32
4.2	Securing DNS	34
4.2.1	Link-Security Approaches	35
4.3	DNSSEC	36
4.3.1	Authenticated Denial	36
4.3.2	DNS-Walk	37
4.4	MLS Based Alternative to DNSSEC	38
4.4.1	Extending Link-Security Approaches	38
4.4.2	Principle of TCB-DNS	39
4.4.3	Computing Link Secrets	42
4.5	The TCB-DNS Protocol	44
4.5.1	The Atomic Relay Algorithm	44
4.5.2	Preparation of TCB-DNS Master File	46
4.5.3	Verification of RRsets	47
4.5.4	Proof of Correctness	50
4.6	Practical Considerations	51
4.6.1	TCB-DNS vs. DNSSEC	52
4.6.2	Authenticated Denial	53
4.6.3	Overhead	55
4.6.4	Replay Attacks	56
4.6.5	DNSSEC with TSIG	56
4.6.6	NSEC3 Opt-Out	57
4.7	Alternative to IPsec	58
4.7.1	IPsec Operation	59
4.7.2	IPsec Issues	60
4.7.3	IPsec Alternative Leveraging TCB-DNS	60
5	Scalable Key Distribution Schemes	63
5.1	Certificates Based Schemes	63
5.2	Identity Based Schemes	64
5.2.1	Identity-Based Key Predistribution Schemes	64
5.2.2	Blom's Schemes	65
5.3	Probabilistic KPSs (PKPS)	67
5.3.1	Allocation of Subsets	67
5.3.2	Random Preloaded Subsets	68
5.3.3	Hash-Chain KPS	68
5.3.4	Hashed Random Preloaded Subsets (HARPS)	70
5.4	(n, p) -Security of HARPS	71
5.4.1	Probability of Winning a Round	72
5.4.2	Optimization of Parameters	73

5.5	Deterministic Versus Probabilistic KPSs	75
5.5.1	KPS Complexity	77
5.5.2	Complexity Versus Desired Collusion Resistance n	78
5.5.3	Using External Resources	78
5.5.4	Low Complexity Hardware	79
5.5.5	Multiple KDCs and Renewal	79
5.5.6	Exploiting Multi-path Diversity	80
5.5.7	Conclusions	80
6	Scalable Extensions of Nonscalable Schemes	81
6.1	Parallel Basic KPS	81
6.2	Parallel Leighton–Micali Scheme (PLM)	82
6.3	(n, p) -Security of PBK and PLM	84
6.3.1	Optimal Choice of Parameters m and M	84
6.4	Subset Keys and Identity Tickets (SKIT)	85
6.4.1	(n, p) -Security of SKIT	86
6.4.2	Optimal Choice of Parameters	87
6.5	Comparison of KPSs	87
6.6	Beyond (n, p) -Security	90
6.6.1	(n, ϕ, p_a) -Security of RPS	91
6.6.2	(n, ϕ, p_a) -Security of PBK/PLM	93
6.6.3	(n, ϕ, p_a) -Security of SKIT	95
6.6.4	Addressing Message Injection Attacks	95
6.7	PLM for Sensor Networks	96
6.7.1	Classical Sensor Network Model	97
6.7.2	Assumptions	97
6.7.3	Key Distribution for Sensor Networks	98
6.7.4	Key Establishment	99
6.7.5	Performance and Overhead	100
6.8	Conclusions	101
7	Using PKPSs with Tamper-Responsive Modules	103
7.1	Core Principles	103
7.1.1	Active and Passive Shields	104
7.1.2	State Transitions	105
7.1.3	Single-Step Countermeasures	107
7.2	The DOWN Policy	107
7.2.1	DOWN-Enabled Modules	108
7.2.2	DOWN with Other Asymmetric Schemes	109
7.2.3	DOWN With ID-Based Schemes	111
7.2.4	DOWN Assurance and Complexity	113
7.2.5	DOWN with PKPSs	114
7.3	A Second Look at Key Predistribution Scheme (KPS) Complexity	114
7.3.1	Generic Device Model	115

7.4	Comparison of KPSs	117
7.4.1	Deployment Complexity	117
7.4.2	Complexity During Regular Operation	120
7.4.3	PLM	122
7.4.4	PBK	122
7.4.5	RPS and HARPS	123
7.5	KPS Algorithms	124
7.5.1	MLS	126
7.5.2	Scalable KPSs	126
7.6	Security Protocols Utilizing $f_{pw}()$	127
7.6.1	Atomic Relay Protocols	128
7.6.2	Atomic Authentication Relay Algorithm	128
7.6.3	Atomic Path Secret Relay Algorithm	130
7.6.4	Accepting Relays	131
7.7	Conclusions	133
8	Broadcast Authentication and Broadcast Encryption	135
8.1	Certificates-Based Broadcast Authentication (BA)	135
8.1.1	One-Time Signatures (OTS)	135
8.1.2	Timed Efficient Stream Loss Tolerant Authentication (TESLA)	137
8.2	Identity-Based Broadcast Authentication (BA) Using Key Predistribution	138
8.2.1	Reducing Signature Size	139
8.2.2	Effect of Decrypt Only When Necessary (DOWN) Assurance	141
8.3	Broadcast Encryption	142
8.3.1	Tree-Based Broadcast Encryption (BE) Schemes	142
8.3.2	Broadcast Encryption (BE) Using Probabilistic Key Distribution	144
8.3.3	Broadcast Encryption (BE) by Sources Other Than Key Distribution Center (KDC)	145
8.4	Performance of Probabilistic Key Predistribution Scheme Broadcast Encryption (PKPS BE)	145
8.4.1	Performance Bounds	147
8.4.2	Over-Provisioning Keys	148
8.4.3	Hashed Random Preloaded Subsets (HARPS) vs. Random Preloaded Subsets (RPS)	149
8.5	Models for Broadcast Encryption (BE)	152
8.5.1	$G = N$ Models	152
8.5.2	$N \gg G$ Models	153
8.5.3	Batch Sizes for External Sources	155
8.6	Application of Probabilistic Key Predistribution Scheme Broadcast Encryption (PKPS BE) in Publish–Subscribe Systems	157
8.6.1	Desirable Features	157

8.6.2	PKPS-BE vs. T-BE for Pub-Sub Systems	158
8.6.3	Pub-Sub Operation	160
9	Authenticated Data Structures	163
9.1	Merkle Tree as an ADS	164
9.1.1	Merkle Tree Protocols	165
9.2	Ordered Merkle Tree	167
9.2.1	OMT Leaves	167
9.2.2	OMT Nodes	169
9.2.3	Verification and Update Protocols	170
9.2.4	Insertion of OMT Leaves	171
9.2.5	Reordering OMT Leaves	173
9.2.6	Index Ordered Merkle Tree	174
9.2.7	Domain Ordered Merkle Tree	175
9.2.8	Summary of OMT Properties	176
9.3	OMT Algorithms in Trusted Resource Limited Boundaries	177
9.3.1	Self-Certificates	178
9.3.2	Core OMT Functions	179
9.3.3	OMT Functions Exposed by T	180
9.3.4	Root Equivalence Certificates	183
9.3.5	Module T State	186
9.3.6	Using Module Functions	188
9.3.7	Context/Application Dependent Functions	189
9.4	Infrastructural Requirements	191
10	Universal Trusted Computing Bases	195
10.1	Practical Systems	195
10.1.1	Complexity and Ignorance	195
10.1.2	System Security Model	197
10.2	Trusted Platform Modules	198
10.2.1	Realizing a TCG Trusted Platform	198
10.2.2	Pitfalls of the TCG Approach	199
10.3	Trinc	200
10.3.1	Virtual Counters	202
10.4	Credential Management Modules	203
10.4.1	Credential Transaction Model	204
10.4.2	Consequential Transactions	207
10.4.3	Virtual Networks	207
10.4.4	VN State Changes	208
10.4.5	CMM State and VN State	209
10.4.6	Changing VN State	210
10.4.7	CMMs as ADS Constructors and Verifiers	211
10.5	CMM System Architecture	212
10.5.1	CMM Universe	213
10.5.2	Creation of Virtual Networks	213

10.5.3	Intra-VN Key Distribution	215
10.5.4	VN Links	215
10.6	Credential Transaction Model of Representative Systems	216
10.6.1	Credential Transaction Model for DNS	217
10.6.2	DNS Transactions	219
10.6.3	Transaction Models for Other Systems	221
11	Conclusions	223
	References	227
	Index	233

Symmetric Cryptographic Protocols

Ramkumar, M.

2014, XVII, 234 p. 21 illus., 1 illus. in color., Hardcover

ISBN: 978-3-319-07583-9