References


SECURE GROUP COMMUNICATIONS OVER DATA NETWORKS


REFERENCES


REFERENCES


About the Authors

Xukai Zou received his B.S. degree in Computer Science from Zhengzhou University, Zhengzhou (China) in 1983, his M.S. degree in Computer Science and Engineering from Huazhong University of Science and Technology, Wuhan (China) in 1986 and his Ph.D. degree in Computer Science from the University of Nebraska-Lincoln in 2000. Before pursuing his Ph.D. degree, Dr. Zou served as an Associate Professor (1994–1998), Assistant Professor (1988–1993) and Lecturer (1986–1987) at Zhengzhou University. Currently Dr. Xukai Zou is an Assistant Professor with Purdue University School of Science at Indianapolis, Indiana, USA. His research interests include applied cryptography and network security, in particular, secure group communication/secured dynamic conferencing, Web technology and Internet engineering, wireless networks, and analysis and design of computer algorithms. Dr. Zou has authored two books and published over ten security-related papers on group/conference key management for secure group communications and secure dynamic conferencing. He has served as a member of a number of technical program committees, member of editorial boards, and a reviewer for many international organizations, international conferences and international journals. He is a recipient of two U.S. National Science Foundation grants. His email address is xkzou@cs.iupui.edu.

Byrav Ramamurthy received his B.Tech. degree in Computer Science and Engineering from the Indian Institute of Technology, Madras (India) in 1993. He received his M.S. and Ph.D. degrees in Computer Science from the University of California (UC), Davis in 1995 and 1998, respectively. Currently Dr. Ramamurthy is an Associate Professor in the Department of Computer Science and Engineering at the University of Nebraska-Lincoln (UNL). At UNL, Dr. Ramamurthy leads the Networking Research Group in ongoing projects on topics such as optical networks, network security, wireless networks, grid computing, and telecommunications. He is the co-director of the UNL Academic Program Priority Initiative in the areas of Simulation & Computing Engineering (SCE) and Information Technology & Telecommunications (ITT). He is the founding co-director of the Advanced Networking and Distributed Experimental Systems (ANDES) Laboratory at UNL. Dr. Ramamurthy is the author of the textbook "Design of Optical WDM Networks - LAN, MAN and WAN Architectures" published by Kluwer Academic Publishers in 2000. He was the Feature Editor on Theses for the Optical Networks magazine. He was a guest co-editor for a special issue of IEEE Network magazine on Optical Communication Networks. He has served as a member of the technical program committees for the IEEE INFOCOM, IEEE GLOBECOM, Opticomm, ICC and ICCCN conferences. From 2001-2003, he served as the founding secretary of the IEEE ComSoc Optical Networking Technical Committee (ONTC). Dr. Ramamurthy was a recipient of the Indian National Talent Search scholarship and was a Fellow of the Professors for the Future program at UC Davis. He was the recipient of the UNL College of Engineering and Technology Faculty Research Award for 2000 and the UNL CSE Dept. Students Choice Award for the Best Graduate Professor for 2002-2003. Dr. Ramamurthy’s research is supported by the U.S. National Science Foundation, Agilent Tech., and OPNET Inc. His email address is byrav@cse.unl.edu.
Spyros Magliveras received his Bachelor's Degree in Electrical Engineering in 1961 and his Master's degree in Mathematics in 1963 both from the University of Florida. He studied for his Ph.D. degree at the University of Michigan under Professor Donald Livingstone from 1964 to 1968. In 1968 he followed his Professor to Birmingham, England, and completed his Ph.D. in Mathematics from the University of Birmingham in 1970. During his studies he was influenced by Donald Livingstone, John H. Conway, Donald G. Higman, Roger C. Lyndon, Marshall Hall, Jr. and Tom Storer. Currently Dr. Magliveras is Professor of Mathematical Sciences and Director of the Center for Cryptology and Information Security at Florida Atlantic University. Prior to his present position, Dr. Magliveras held the Distinguished Henson Chair for Communication and Information Theory at the University of Nebraska-Lincoln (1991-2000) and earlier academic positions at the University of Nebraska - Lincoln (1978-1991) and the State University of New York (1970-1978). His research interests include cryptology, network security, data compression, finite groups, combinatorics, the design & complexity of algorithms, and finite geometry. He has been working on group-theoretic cryptography for over two decades and is becoming increasingly interested in approaches based on combinatorial group theory. He has served on many professional committees and boards, has organized several International Conferences and served on several editorial boards. He has received numerous awards and sponsored research grants and holds a U.S. patent for a cryptosystem. He was awarded 8 prizes and honors including The ICA Euler Gold Medal Award for research in combinatorial mathematics. He has presented over 100 papers in International Conferences, has published over 80 papers in International Journals and the Proceedings of International Conferences and has edited four technical volumes. His email address is spyros@fau.edu.
The authors welcome your comments and suggestions about this book. Please send them to the following addresses:

Prof. Xukai Zou
Department of Computer and Information Science
Purdue University School of Science at Indianapolis
723 W. Michigan ST. SL280E
Indianapolis, IN 46202, U.S.A.
Phone: (317) 278-8576
Fax: (317) 274-9742
Email: xkzou@cs.iupui.edu
Web: www.cs.iupui.edu/~xkzou/

Prof. Byrav Ramamurthy
Department of Computer Science and Engineering
University of Nebraska-Lincoln
256 Avery Hall
Lincoln, NE 68588-0115, U.S.A.
Phone: (402) 472-7791
Fax: (402) 472-7767
Email: byrav@cse.unl.edu
Web: www.cse.unl.edu/~byrav/

Prof. Spyros Magliveras
Department of Mathematics Sciences
Florida Atlantic University
Boca Raton, FL 33431, U.S.A.
Phone: (561) 297-0274
Fax: (561) 297-2436
Email: spyros@fau.edu
Web: www.zeus.math.fau.edu/spyros/
Index

AKD, 137, 139
AKT, 73
ALX Tree, 135
Access Control, 3
Access Grid, 150
Access Point, 131–132
Ad Hoc Network, 131, 135, 140, 145–148
Admission Control, 3, 24, 149
Aggregate Operation, 14, 52–55
Akl-Taylor Scheme, 109–112
Area Key Distributor
See AKD
Area Key, 137–139
Area Threshold, 139
Asymmetric Cryptosystem, 9, 11
Authenticated Diffie-Hellman, 12, 79
Authentication, 1–2, 125–126
Auxiliary Key Tree
See AKT
Auxiliary Key, 73–74
BD Protocol, 39
BF-TGDH DC, 101, 149
BF-TGDH, 50, 78–80, 82, 101
Back-End Key, 78–79
Dummy Blinded Key, 80
Dummy Component, 79
Dummy Member, 79
Dummy Private Share, 79
Dummy Public Share, 79
Dummy Root Key, 79–80
Dummy Secret Key, 80
Front-End Key, 78
BS, 131–133, 146
BS-Subtree, 133, 135
Back-End Key, 78
Backbone Key, 141
Backbone, 141, 143–145
Background, 78, 81
Backward Secrecy, 69, 134, 136–137, 139
Base Station
See BS
Baseline Rekeying, 137–138
Basic Interval, 96–100
Battery Power, 146
BiBa, 130
Bijection, 10
Bin Ball, 130
Binary Key Tree, 59
Bit-string, 54
Blinded Key, 81, 83, 85–89
Block-Free Tree Based Group
Diffie-Hellman Scheme
See BF-TGDH
Boolean Function Minimization, 73, 75
Boolean Membership Function, 75
Boolean Monomial, 75
Bottleneck, 146
Broadcast Authentication, 130
Broadcast, 1, 8
Bulk Leave, 73
Bulk Operation, 13–14, 49, 52, 134
Bursty Behavior, 13, 49, 52, 95
Bursty Operation, 13–14, 49–50, 52
CA, 11
CBT, 23–24
CLIQUES, 2
CRT, 3, 6, 93, 106, 122–123, 125–126
CRTHACS, 122, 125–126
Cellular Network, 131–132
Central Authority, 146
Central Trusted Server, 92
Certificate Authority
See CA
Certificate, 11
Chinese Remainder Theorem Based Hierarchical Access Control Scheme
See CRTHACS
Chinese Remainder Theorem
See CRT
Ciphertext Space, 7
Ciphertext, 7, 119
Cluster Key, 29, 31–33, 141–142, 145
Cluster Leader, 28, 30–33
Cluster, 28
Clusterhead, 142–145
Clustering Protocol, 28–31, 33, 36
Coefficient, 59, 94, 96
Collaborative Work, 1
Collision Resistant, 4
Communicant, 2, 11
Complexity, 4, 93, 96, 103, 118, 125
Communication Complexity, 118–119, 125
Space Complexity, 4, 93, 96, 103, 118, 125
Time Complexity, 4, 93, 96, 103, 118, 125
Computational Security, 4
Computationally Infeasible, 10, 20, 114, 120
Conference Key, 99, 102–103
Conference, 3, 91, 98
Congruence, 6
Contributory Group Key, 37
Contributory Protocol, 147
Coordinator, 45–46
Core Based Tree
See CBT
Core Tree, 23
Cryptographic Hash Function, 3
Cryptology, 1
Cryptosystems, 8
Cumulative Member Removal, 73
Cyclic Multiplicative Group, 5
D-Ary Key Tree, 59
DAG, 106–107, 113
DEK, 22–23, 26–28, 76, 80–81, 136–137
DEP, 25–27
Key-Subgroup Key, 26
Key-Subgroup, 26
Subgroup Key, 26
Subgroup, 26
DH Key, 12
DHP, 12
DISEC, 50, 83–84, 87–88
Blinded Key, 83
Key Distribution Binary Tree, 83
Key Node, 83
Node Secret, 83
Unblinded Key, 83
INDEX

Distributed Scalable Secure Communication
See DISEC
DKD, 136–137
DLP, 3, 5–6, 11–12, 20
Data Encryption Key
See DEK
Decryption Function, 120
Decryption Rule, 7
Decryption Transformation, 10
Delayed Rekeying, 137–139
Deterministic Algorithm, 7
Diffie-Hellman Disguised Public Share, 12, 76
Diffie-Hellman Key Exchange, 5, 11–13, 37, 76, 79
Diffie-Hellman Key, 76, 81
See DH Key
Diffie-Hellman Private Share, 12, 76
Diffie-Hellman Problem
See DHP
Diffie-Hellman Share Generator, 79
Diffie-Hellman, 30
Directed Acyclic Graph
See DAG
Directed Multicast, 9, 59, 63–64
Directly Dependent Key Scheme, 106, 109
Discrete Logarithm Problem, 5
See DLP
Disjunction, 75
Distributed Binary Key Tree, 84
Distributed Interactive Simulation, 1
Domain Key Distributor, 136
See DKD
Domain, 136–137
Dual Encryption Protocol
See DEP
Dummy Blinded Key, 80–81
Dummy Component, 79
Dummy Member, 78–80, 95
Dummy Number, 95
Dummy Private Share, 79
Dummy Public Share, 79
Dummy Root Key, 79–80, 82
Dummy Secret Key, 80–81
EKOL, 139
ElGamal Public-Key Cryptosystem, 5
ElGamal Signature Scheme, 5, 80
ElGamal Signature, 79
Elliptic Curve, 5
Encryption Algorithm, 93
Encryption Function, 119, 121
Encryption Rule, 7
Encryption Transformation, 10
Encryption, 2
Ethernet, 144
Euclidean Algorithm, 5
Euler’s $\phi$ Function, 7
Exponential Back-Off Algorithm, 144
Exponential Delay Parameter, 144
Extended Euclidean Algorithm, 21, 112
Extra Key Owner List
See EKOL
Factorization, 7
Finite Field, 5, 20
Forward Secrecy, 69, 136
Front-End Key, 78
GCD Attack, 119, 125
GCD, 119
GDH, 39
GDH.1, 39
GDH.2, 41
GDH.3, 42
GI, 23
GSA, 25
GSC, 25, 135
GSEC, 1
GSI, 25
Generator, 5, 11, 20, 37
Greatest Common Divisor Attack
See GCD Attack
Greatest Common Divisor
See GCD
Group Communication, 1–2, 18
Broadcast Communication, 18
Few-To-Many Communication, 18
Many-To-Many Communication, 18, 20, 49
Multicast Communication, 18, 20–21
One-To-Many Communication, 18, 20, 22, 26, 28, 49
Group Controller
See GC
Group Diffie-Hellman
See GDH
Group Dynamics, 2, 13, 95
Group Identity Key, 141
Group Initiator
See GI
Group Key Management, 2–3, 13–14, 17, 49, 66, 73, 127, 132, 135, 145, 149
Centralized Key Distribution, 18, 20, 49–50
Contributory Key Agreement, 18, 20, 49
Distributed Key Agreement, 18, 20, 49–50, 76
Public-Key Based Key Management, 20, 23
Secret-Key Based Key Management, 23
Group Key, 2, 17
Group Merge, 14
Group Partition, 14
Group SECUrity
See GSEC
Group Security Agent
See GSA
Group Security Controller
See GSC
Group Security Intermediate
See GSI
Group Splitting, 14
Group-Oriented Rekeying, 59, 63–64
Group-Oriented, 63
HELLO Message Encryption Key, 141
Hand-Off, 134
Hash Function, 3, 46, 74–75, 129
Hierarchical Access Control, 149
See HAC
Horus/Ensemble, 2
IDC, 101
IETF, 1, 9
IHACS, 114, 119, 121
ING Protocol, 37
IP Multicast, 8
IP, 1
IRTF, 1
ISP, 25
Immediate Rekeying, 137–138
Index Based Hierarchical Access Control Scheme
See IHACS
Indirectly Dependent Key Scheme, 106, 112
Integrity, 2
Inter-Area Rekeying, 137
Interactive Game, 1
Internet Engineering Task Force
See IETF
Internet Protocol
See IP
Internet Research Task Force
See IRTF
INDEX

Internet Service Provider
See ISP

Interruption, 78, 81–82

Interval Based Dynamic
Conferencing, 97–98

Interval Communication, 96

Interval Multicast, 96

Interval, 96–97, 99, 103

Intra-Area Rekeying, 137

Intractability, 5

Isomorphic, 5

K-Resilient Security, 4, 19

KAG, 85–87, 89

KDC, 23

KEK, 23, 27–28, 50

Karnaugh Map, 75

Key Agreement, 2, 147

Key Association Group
See KAG

Key Distribution Binary Tree, 83

Key Distribution Center
See KDC

Key Distribution, 92, 146

Key Encryption Key
See KEK

Key Graph, 49

Key Management, 2–3, 15, 91

Key Manager, 144

Key Node, 83

Key Server, 29–30, 32

Key Tree, 19, 49–50, 54, 57, 65–66,
73, 76–77, 82, 84, 91, 96–99,
102, 106, 122, 132, 150

Key-Oriented Rekeying, 59, 64

Known Plaintext Attack, 119

LAN, 8

LKH, 49–50, 65–67, 69, 72–73, 132,
137

LSK, 26–28

Lagrange Interpolation, 5

Layer Key, 29–33

Leader, 30

Lin’s Scheme, 112

Local Area Network
See LAN

Local Subgroup Key
See LSK

Logarithmic Signature, 121

Logical Key Hierarchy
See LKH

Logical Key Tree
See LKH

MAC, 124–125, 142

MID, 73

MSA, 3, 79, 130, 149

MSEC, 1

Man-In-The-Middle, 11–13, 79

Master Keys, 111

Matching Resistant, 3

Member Discovery Protocol, 33–34

Member Dynamics, 2, 115, 117, 122,
125

Member Exclusion List, 23

Member ID
See MID

Member Inclusion List, 23

Member Overlay Tree, 33–34, 36

Member Serialization, 37

Member-Oriented Rekeying, 59–60,
62, 64

Member-Oriented, 62

Membership Control, 23

Membership Management, 3, 149

Message Authentication Code
See MAC

Message/Source Authentication
See MSA

Mixed Keying, 106–108

Mobile Station, 131

Mobility, 147

Modern Cryptology, 1
Modular Exponentiation, 119
Modulo, 6
Multicast Delivery Tree, 9
Multicast SECurity Working Group  
See MSEC
Multicast Tree, 9, 21, 23, 33
Multicast, 1, 8  
   Directed Multicast, 9  
   Multiple Multicast, 9  
   Scoped Multicast, 9  
   Subgroup Multicast, 9
Multiple Multicast, 9
Multiplicative Group, 7, 11
Multiplicative Inverse, 6, 21, 112
N-Party Diffie-Hellman Key  
   Exchange, 18, 37, 149
Neighboring Comparison, 56, 99
Neighboring clusterhead discovery, 143
Node Key, 65–66, 68, 83
Non-Occupied Position, 95
OFC, 49–50, 66, 68–69
   Node Secret, 66
OFT, 49–50, 65–66, 68–72, 83
   Blinded Node Secret, 65
   Blinded Node Secret, 65–66
   Node Key, 65–66
   Node Secret, 65–66
Off-Line, 79–80, 92–93, 102
One-Way Function Chain  
See OFC
One-Way Function Tree  
See OFT
One-Way Function, 3–4, 6, 15, 20,  
   49, 65–66, 76, 79–84, 105–106,  
   108, 112–115, 119, 141
One-Way Hash Function, 3
One-Way-Function Tree, 49
Outsider, 1
PGM, 121
PKDC, 149
PKI, 137
PKM, 144
PKMs, 144
POF, 79–80
Pairwise Key, 29
Participant, 1–2
Pebble Network  
See Pebble Network
Pebble, 140
Pebblenet, 140, 142
Periodic Rekeying, 14, 137, 139
Permanent Private Share, 80
Permutation Group Mapping  
See PGM
Permutation, 8
Plaintext Space, 7
Plaintext, 7, 119
Poisson, 135
Potential Key Manager, 144
Primitive Element, 5
Privacy, 1
Private Key, 7
Private Share, 12, 45, 76–79
Privilege, 105
Probabilistic Algorithm, 7
Public Directory, 10
Public Key Based Scheme, 92
Public Key Certificate, 11, 13
Public Key Infrastructure  
See PKI
Public Key, 7, 23
Public One-Way Function  
See POF
Public Share Certificate, 13
Public Share, 12, 45, 76–79
Public-Key Based Scheme, 18
Public-Key Based System, 4
Public-Key Cryptosystem, 7, 9–11,  
   17–20, 22, 93, 102–103, 125
Published Diffie-Hellman, 12–13, 79
Pure Delayed Rekeying, 139
RPS, 20–22
INDEX

RSA Cryptosystem, 7
RSA Signature, 79
RSA, 7, 21
Rampart, 2
Random Number Generator, 120–121
Real-Time Information Service, 1
Rekeying, 24
Relaying Message, 24
Resource Multiple Keying, 106–108
Reversible Parametric Sequence
See RPS
Root Key, 82
SGC with HAC, 2–3, 15, 105
SGC with Hierarchical Access Control
See SGC with HAC
SGC, 1, 3–4, 6, 8, 13–15, 17, 37, 49, 66, 72, 91, 105–106, 140, 145, 149
Lightweight, 131
SGCS, 4
SGM, 19, 25–26
Member SGM, 26–27
Participant SGM, 26–28
SH, 132–134
SK, 22, 73–74, 92–93
SLDC, 149
SMuG, 1
SPREAD, 2
STB, 20, 22–23
STPC, 1–2
STR Protocol, 45
Scoped Multicast, 9
Secret Key, 10–12, 81
Secret Share, 95
Secret Sharing, 7
Secret-Key Based Scheme, 19
Secret-Key Based System, 4
Secret-Key Cryptosystem, 9–11, 19, 23, 102, 121
Secure Group Communication Scheme
See SGCS
Secure Group Communication
See SGC
Secure Lock, 6, 93–94, 102–103
Secure Multicast Research Group
See SMuG
Secure SPREAD, 2
Secure Transmission Backbone
See STB
Secure Two-Party Communication
See STPC
SecureRing, 2
Security Requirement, 14
Backward Secrecy, 14–15
Forward Secrecy, 14
Sensor Network, 146
Serialization, 45, 147
Session Key
See SK
Shadow, 4
Shadowholder, 4
Shareholder, 5
Shares Generator, 79
Signatures, 2
Single-Point-Of-Failure, 146
Source Heartbeat Message, 34
Split Operation, 52
Sponsor, 77–78, 81–82
Square-Multiply, 119
Steer Protocol, 43
SubGroup Manager
See SGM
Subgroup Controller, 106, 118, 123, 125
Subgroup Dynamics, 115–116, 122, 125
Subgroup Key, 19
Subgroup Multicast, 9, 59–60, 63–64
Subgroup, 19, 24, 105, 113, 122
Supervisor Host
See SH
Symmetric Cryptosystem, 9–10, 19, 23
Symmetric Polynomial, 3, 7–8, 94–96, 102–103
TA, 17
TEK, 50, 141, 143–144
TESLA, 130
TGDH, 50, 76, 78–80, 149
Blinded Key, 76–78
Secret Key, 76–77
TIKM, 132
TMKM, 132, 134, 139
TTL, 87
TTL-Scoped Heartbeat Message, 34
TTL-Scoped Message, 34, 36
Tamper-Resistant, 141, 145
Tele-Medicine, 1
Teleconferencing, 1
Threshold Cryptosystem, 4–5
Threshold Rekeying, 139
Time-To-Live
See TTL
Timed Efficient Stream Loss-Tolerant Authentication, 130
Topology Independent Key Management
See TIKM
Topology Matching Key Management
See TMKM
Traffic Encryption Key
See TEK
Transformation, 10
Tree Based Group Diffie-Hellman Scheme
See TGDH
Tree-Based Key Management, 17
Tree-Based SGC Key Management, 15
Trusted Authority
See TA
Two Party Diffie-Hellman Key Exchange, 76
Two-Party Communication, 2
Unblinded Key, 83–84, 87–89
Unconditional Security, 4
Unconditionally Secure, 4, 19, 92, 94, 101–102, 105–107
User Multiple Keying, 106–107
User Threshold, 139
User-Oriented Rekeying, 59
User-Subtree, 133, 135
VPN, 1, 150
Virtual Private Network
See VPN
WAN, 150
WLAN, 131
WPAN, 131
WTBR, 134, 139
WWAN, 131
Wait-To-Be-Removed List
See WTBR
Weight, 142, 144
Wide Area Network
See WAN
Wireless Local Area Network
See WLAN
Wireless Network, 130–131
Wireless Personal Area Network
See WPAN
Wireless Wide Area Network
See WWAN